Advisory Board | Health Care IT Advisor

The best practices are the ones that work for you.℠

Research Brief

Rising to Prominence in the New Security Landscape: Health Care's Chief Information Security Officer

The escalating financial stakes and sheer volume of cyberattacks have elevated the role of the Chief Information Security Officer (CISO) in health care organizations (HCOs) to a leader central to the organization's ability to fulfil its mission to care for patients. No longer is the CISO a purely technical role—now, HCOs entrust their CISO to protect the entire business enterprise through holistic risk mitigation.

Executive Summary

Problem: A New Cyber Landscape

HCOs now must contend with highly organized, professional threat actors using increasingly sophisticated and powerful tools—no longer will the CISO of yesteryear effectively protect the organization. This fast-changing cyber landscape demands a reexamination of the role.

Context: A Set of New CISO Requirements

Empowered, technically competent, strategic-thinking, and risk-focused security leaders with full organizational support are required to shepherd the organization toward an advanced and adaptive security posture. A great CISO is technically skilled, of course, but also a strong leader with sharp business acumen (risk-focused), and a bit of a politician to get things done.

Analysis: Key Elements of a Great, Effective CISO

Several considerations for the CISO role can impact the CISO's effectiveness and ability to advance the organization's security posture. Key considerations include appropriate organizational model, CISO placement relative to IT, reporting structure, level of role, and level of responsibilities outside of IT. HCOs must find the right mix of answers to these considerations that matches their organizational culture, security maturity, and short- and long-term security priorities. Organizations that have effective CISOs who stay for the long term approach security as a team sport, do not place blame or point fingers at individuals, and actively empower their CISO with the authority, and support to enact change.

Action Items: Focus on Partnerships and Empowerment

- Carefully consider how the organization can optimize its CISO's effectiveness.
- Foster effective partnerships and open lines of communication amongst organizational leadership (IT and non-IT leadership).
- Empower your CISO to hold effective boardroom conversations and promote change in the organization's security culture.

Author: Allyson Vicars | January 2018

Evolving Role of the CISO

As cybersecurity risk and awareness amongst C-suites and boards has grown, the role of the CISO has risen in prominence and evolved dramatically over the last decade, especially accelerating in the last few years. Not too long ago, the organization's CISO was likely referred to as the "security guy or gal" and was often buried somewhere within the IT department. Unfortunately, these CISOs—given their myriad other responsibilities and highly technical backgrounds—often focused too heavily on the technical components or approached cybersecurity with more of a "check-the-box" mentality.

Now, HCOs must contend with highly organized, professional threat actors using increasingly sophisticated and powerful tools and techniques—no longer will the old ways effectively protect the organization. This fast-changing cyber landscape demands a re-examination of the role. Empowered, technically competent, strategic-thinking, and risk-focused security leaders with full organizational support are required to shepherd the organization toward an advanced and adaptive security posture.

Leading organizations are beginning to (or already) employ CISOs who approach security from a risk perspective as well as demonstrate a keen business sense and technical wherewithal to operationalize the security strategy. A holistic approach to security encompassing areas of governance and policy, process and education, and technical components is key for all HCOs.

Organizational Models

HCOs manage administrative and technical security functions in a variety of ways. Three common organizational models are illustrated below. ***Whichever model is chosen, it is critical that it aligns with the entire organization, not solely the IT department***. Doing so ensures security functions are considered as part of all activities and decisions.

- The **distributed model** spreads administrative and technical functions across different areas of the organization. For example, the help desk handles provisioning, network administration handles engineering, internal audit handles audits, and compliance handles security officer duties, policy setting, and risk assessments.
- The **divided model** splits administrative and technical functions between two individuals, often from different departments. An individual from the compliance, legal, or audit departments commonly manages the administrative activities—such as governance and policy management, audit and compliance tracking—leaving the technical functions of security—such as provisioning, firewall administration, intrusion protection management, etc.—to an individual within the IT department.
- The **centralized model** is the most prevalent form within larger health care organizations. Both administrative functions (including policy setting, risk assessments, and audits), as well as technical functions (such as IAM[1] provisioning, and engineering), fall to a single individual known as the security officer.

[1] IAM = Identity and access management.

Author: Allyson Vicars | January 2018

Key CISO Considerations

Carefully consider how CISO placement and reporting structure, level of role, and inclusion of other responsibilities could impact the organization's security posture and ability to adapt to changing security needs.

The organization's needs for and from a CISO will change over time as the organization's posture evolves, so ensure these considerations are reviewed as needed to maintain continued alignment and on-going effectiveness.

Key Considerations

Must Match Security Culture and Goals of Your Organization

CISO Placement and Reporting Structure

Placement Within the Organization

Key Takeaway:

Effective security management and oversight comes down to effective partnerships between security and IT, as well as between security and non-IT leadership who recognize and own their accountability for cybersecurity preparedness.

Our health care provider interviewees across the 2017 research cycle (predominantly CIOs) expressed a strong and consistent preference that the CISO should reside within the IT department, citing two main reasons: (1) much of the technical work would fall on IT anyway; and (2) CISOs tend to be highly technical individuals who would feel best supported within the IT department.

While these are valid points and worthy of consideration, IT leaders should recognize that the placement of the CISO within the organization has implications for the CISO's ability to impact change on the security culture and posture of the organization and, perhaps most importantly, it has implications for how the C-suite approaches their role in cybersecurity.

Typically, the more advanced and robust the organization's security culture, the further away from IT the CISO can sit and still function effectively. Ideally, the CISO will be as closely aligned as possible with key organizational priorities. For example, if innovation is critical, the more closely aligned the CISO should be with that business group.

A CISO external to IT can be a budget benefit.

One benefit of housing information security outside of IT is that it often means an entirely separate budget to support security initiatives instead of it being a line item in the IT budget. Given the interconnectedness of IT and security, this provides an opportunity for flexibility, negotiation, and sharing of funds between the two departments for certain projects as needs throughout the year change. Regardless of structure, effective security management comes down to effective partnerships.

Author: Allyson Vicars | January 2018

CISO Reporting Structure

66%

Percentage of health care CISOs who currently report to their CIOs

Reporting structure is one of the more politically sensitive and debated topics of security leadership. As the role continues to evolve beyond one that is purely technical into one focused on risk management and protecting the entire business enterprise, reporting lines are evolving concurrently. According to a 2017 study from security firm Symantec and HIMSS Analytics, 66% of health care CISOs report to their CIOs.[2] While it makes sense for CISOs to report to CIOs given the technical nature of parts of the role, one cannot ignore that there may be moments when IT leaders may want to prioritize completing a project over its security implications, thus creating a potential conflict of interest. It may also send the wrong message to the organization that security is a purely technical problem and function.

External to health care, CISOs tend to report to leadership outside of IT, and in some cases directly to the CEO (often the case within the financial services industry) or to legal department leadership. Sentiment among security professionals across all industries is that it will become more prevalent for CISOs to report to the CEO as security continues to increase in importance. Certainly, not all CEOs have the time or appetite for another direct report, so this may not be a viable option for everyone. Counter to this, some organizations have moved the CISO as far as two levels below the CIO. One arrangement we have heard of is having the CISO report to the CTO, who reports to the CIO.

The right choice for each organization will depend on how dramatically leaders want to change the organization's security culture, how cyber-literate its non-IT leaders are about cyber risks, and what the organization's culture is regarding security (total lock down versus looser controls).

Positioning of the CISO and the kind of CISO needed will change over time.

CISO reporting structure is often reconsidered in the event of breach remediation. We are aware of a few instances in which the CISO was reorganized to report directly to the CEO as part of remediation following a major data breach. As time passed and the organization experienced leadership turnover, the CISO reporting structure reverted to reporting directly to the CIO. The positioning of the CISO or even the kind of CISO needed in the organization will change over time.

Case in Brief: Parkview Health's Dual CISO Reporting Structure

Key Takeaway:

Alignment of motivations among leaders will always trump and outperform official reporting lines.

Parkview Health in Fort Wayne, Indiana recognized a need to elevate the organization's information security considerations and ensure it is consistently prioritized effectively. They use a **dual reporting structure** as illustrated below. Their CISO resides within the IT department and reports directly to the CIO, who reports directly to the CEO. As an additional safeguard, the CISO has a "dotted line" reporting relationship outside of IT to their general counsel, who also reports directly to the CEO. For Parkview Health, they feel this reporting structure fulfills two important roles:

- Ensures the CIO and CISO have an effective partnership rather than an adversarial or sycophantic relationship
- Provides increased visibility for the C-suite into security efforts

1) Operationalizing Cybersecurity in Healthcare Organizations, Symantec and HIMSS Analytics, 2017.

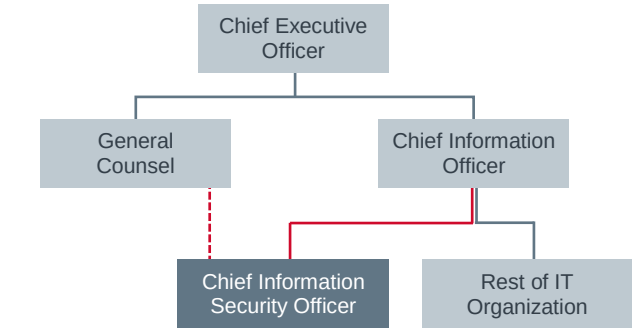
Author: Allyson Vicars | January 2018

This arrangement is not without its own set of difficulties and challenges. It works for Parkview Health, but it is important to note that ***aligned motivations amongst key leaders will outperform any official reporting structures.*** It is imperative that organizations ***carefully scope and define the dotted-line relationship beforehand***. Questions to answer include:

- Which manager will make which decisions?
- What sort of reporting will be shared with the dotted-line manager? At what cadence?
- How will disagreements be resolved?
- What is an agreed-upon escalation plan and path?

Case in Brief: Parkview Health

- Non-profit, eight-hospital health system and medical group based in Fort Wayne, IN
- CIO and CISO lead a strong and consistent effort for transparency on cybersecurity issues
  - Dual reporting structure for CISO who can go to someone outside of IT if feeling things are going astray
- Information security presentations are made to multiple board committees annually, creating an environment in which several board members hear messages multiple times
  - Standing agenda item on the board IT committee (quarterly); agenda item with audit and compliance committees



Avoids a "fox watching the hen house" situation

Provides visibility for C-suite into security efforts

Carefully scope and define dotted-line relationship

Aligned motivations amongst key leaders outperform official reporting structures.

Executive- or Non-Executive-Level Role

Historically within health care, the role of the CISO has not been one of an executive-level leader; however, as cybersecurity awareness grows amongst C-suite and board executives, support for a security-focused executive (separate from the CIO) also grows. The decision here (executive or non-executive role) can impact how the organization as a whole will approach information security.

An executive-level CISO may encourage a more risk-based approach to security—the CISO can view his or her role as one of protecting the business through mitigating risk down to an acceptable level. A non-executive-level CISO may take a more myopic approach and focus more intently on the technology and favor extremely tight security controls that may be at odds with what is feasible operationally or strategically.

Author: Allyson Vicars | January 2018

HCOs that seek dramatic changes in their security culture and posture should consider giving the CISO a seat at the executive table so they can better align security approaches with the strategy of the organization.

Non-Security Responsibilities

Many organizations consider giving the CISO responsibilities that fall outside of security to ensure they keep a broader approach and understand the implications of their security controls and policies. A CISO focused on nothing but security or reporting to someone with no line responsibilities, such as the compliance officer, may lead them to constantly criticize everything and resist change as they could take their role as needing to eliminate all risk, rather than tuning the level of risk to what the organization is willing to accept.

In today's world this has regulatory implications. Any risk identified as significant by the CISO, such as through a financial audit report or a Meaningful Use risk assessment, will need to be addressed. If they are prone to finding significant risks everywhere, the organization may see a continually growing and unmanageable list of risks to address that may conflict with or hinder their strategic efforts. In contrast, charging a CISO with getting things done outside of security may weaken security efforts as the CISO may value "getting things done" over keeping things secure.

HCOs must strike the right balance for their CISO. If these symptoms are present, the organization may wish to consider combining the CISO with another role—such as making the CIO or CTO the CISO—or they could consider giving the CISO more authority to enact change.

CISO Selection

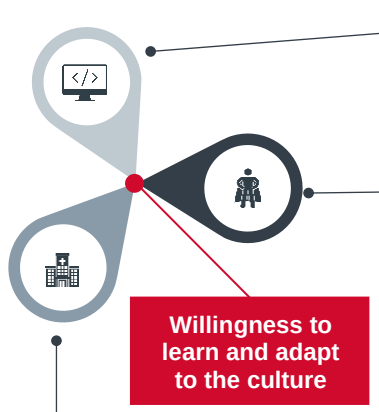
An HCO's CISO will be integral to its information security efforts, so it matters who you put in the role. A great, effective CISO has been described as having a combination of traits rarely found in one person: they must be **technically skilled**, of course, but also a **strong leader** with sharp **business acumen** (risk-focused), and a bit of a **politician** to get things done. A strong **willingness to learn and adapt** underpins these top characteristics, not only because it is necessary in such a rapidly changing landscape, but because ***HCOs should look for candidates who seek to learn the needs and culture of the new organization, then craft security plans that fit those needs.***

At a Glance: Key Attributes to Screen for in a CISO Candidate

- Technically and politically adept
- Clear understanding of risk as an issue of degrees rather than an absolute
- Imbued with native curiosity about how things work and why they the way they are
- Capable of understanding and articulating business and clinical implications
- Level-headed, capable leader in a crisis
- Knowledgeable about legal and regulatory issues
- Willingness to learn and adapt

Author: Allyson Vicars | January 2018

Who You Put in the Role Matters



Technical Ability

- Exhibits a native curiosity about how things work

Leadership Skills

- Paints a clear and convincing vision of security without technical complexity
- Is a capable and level-headed leader in a crisis
- Sees negotiation as a necessary component for advancing security in the organization
- Gets things done through formal and informal channels

Willingness to learn and adapt to the culture

Business Savvy

- Approaches risk as an issue of degrees, not an absolute
- Understands business, clinical, legal, and regulatory implications

A September 2016 survey of security personnel revealed that the top contributing factors for CISO turnover included a lack of a serious cybersecurity culture (31%), a lack of active participation with executives (30%), and higher compensation offered elsewhere (27%).[3] ***HCOs should be candid about the organization's environment throughout the interview process so the CISO candidate fully understands what he or she may be walking into with this position***.

Available in Appendix: a sample list of role responsibilities for a CISO job description.

CISO Empowerment

Whomever the organization chooses as their CISO has to be given a real chance to succeed. Unfortunately, average CISO tenure (across all industries) is short—17 months according to a 2015 study.[4] Though there may have been some improvement in this figure since then, turnover at this rate is detrimental to an organization's security program and can impede any real progress. Security efforts may stall while a new search occurs and while the new CISO learns the organization, important decisions may be deferred, and/or time could be lost due to changes in strategic direction.

Organizations that have effective CISOs who stay for the long term approach security as a team sport and do not place blame or point fingers at individuals when something happens. As the contributing factors for CISO turnover outlined in the previous section indicate, C-suite and board interest and engagement in cybersecurity affairs are a critical component to empowering your security leader.

[3] The State of Cyber Security Professional Careers, ISSA.org, September 2016.
[4] The Average CISO Tenure is 17 Months – Don't be a Statistic!, CIO.com, September 2015.

Author: Allyson Vicars | January 2018

HCOs can further empower their CISO by preparing him or her for the boardroom, such as through the use of an **executive mentor**. This technique can help shape a CISO's mindset from "*preventing all risk*" to "*mitigating organizational risk*." This is a technique The Advisory Board Company used: our CEO spent one-on-one time with our CISO to ready him for board-level discussions. Applying a similar model can bring several positive results:

- Readies CISO for board-level discussion in a safe space
- Refines the language of any presentation to exclude confusing technical jargon or descriptions and can help the CISO present content that will resonate with other C-suite and board members
- Builds in an ally within the boardroom who has a more in-depth understanding of cybersecurity

Related Resource:

Security and the C-Suite
National Meeting Recap Web Conference
Live: Thursday February 15, 2018 at 3:00 PM ET
Available on-demand afterward

Virtual CISO Option

Organizations can struggle to fill or retain a CISO or other security roles for a variety of reasons including location, market, or limited resources to dedicate to security. A viable option for HCOs with this struggle is the virtual CISO model offered by several well-established security vendors. **NorthBay HealthCare** in Fairfield, California is one of several Advisory Board members that has expressed a positive experience using a virtual CISO. After some fine tuning of the partnership, the organization's IT leadership feels they have been able to achieve a higher level of security than they would have trying to staff it or manage it on their own. Below are a few considerations for HCOs weighing this virtual option.

Case in Brief: NorthBay Healthcare

- Two-hospital health system with a 100+ physician medical group based in Fairfield, CA
- Outsource the majority of their security functions to a trusted vendor, Sword and Shield, to gain a depth of coverage likely unattainable with the current size of their security team
- Virtual CISO reports to their Director of Network Operations, who functions as the official CISO for HIPAA
- Able to leverage specialized skills on the vendor side depending upon the needs of

Considerations for a Virtual CISO Model

Establish a Collaboration Approach

Take time to learn about each other and develop communication and report-sharing patterns that meet the organization's specific needs.

Set Clear Service Expectations from Start

Specify the scope of work and services and fine tune an agreement on the deliverables.

Identify a Main Point of Contact (POC) at the Vendor

Use a main POC to improve the vendor's understanding of the organization's culture, people, and processes. This will allow for better coordination of appropriate resources.

Author: Allyson Vicars | January 2018

Action Items

As organizations seek to refine and advance their approach to cybersecurity, we encourage CIOs and other leaders to consider the following:

- **Carefully consider how the organization can optimize its CISO's effectiveness.** Tweaks and changes to the organizational model, reporting structure, leadership level, and CISO responsibilities may provide the CISO with a much-needed boost to enact significant and swift change within the organization's security culture.
- **Engage non-IT and non-security leadership in the cybersecurity conversation.** C-suite and board leadership must recognize that while they can delegate the day-to-day responsibilities of cybersecurity preparation, they cannot delegate accountability for preparing the organization against its cyber risk. Their reaction to security preparation (and incidents) significantly impacts the CISO's ability to make changes in the organization's security efforts and ultimately the organization's ability to retain strong security leadership.
- **Foster effective partnerships and lines of communication amongst organizational leadership.** Security is a balance between risk and operations with two-way communication between security (and IT) and other parts of the organization being key.
- **Empower your CISO to hold effective boardroom conversations and promote change in the organization's security culture.** Consider if using an executive mentor or other technique can build a stronger relationship between the CISO and the board, better prepare the CISO for board-level conversation, and create more informed senior decision makers.
- **Consider a virtual CISO model if your organization has had difficulties maintaining a CISO due to market, location, or resources available, or if it could be used as a means of upgrading their CISO function.** If this model is of interest for your organization, leverage the expertise on the vendor side by focusing on an open, collaborative approach supported by predefined service expectations.

Author: Allyson Vicars | January 2018

Appendix

Sample CISO Responsibilities

The exact recipe of job responsibilities will vary by organization according to need and culture. Below is a pick list of sample CISO role responsibilities for HCOs interested in writing or revising their CISO job description.

- **Risk Management**
  - Work with organizational leaders to establish an acceptable level of risk for the enterprise and for specific initiatives
  - Assess current security against this level of risk
  - Develop strategy and implementation plan to ensure the enterprise achieves the acceptable level of risk
  - Develop a security governance structure and process
  - Ensure regular risk assessments are performed, and risks are tracked and corrected
  - Manage vendor relationships and associated risk
- **Technical Skills**
  - Lead identity and access management, user provisioning, and de-provisioning functions
  - Lead incident response teams
  - Lead investigations into security-related incidents and anomalous activity
  - Ensure the development and maintenance of a resilient security architecture including considerations of technologies such as encryption, network access control, network access device, intrusion detection software, firewalls, anti-virus, virtual private network (VPN), mobile device management software, etc.
- **Policies and Procedures**
  - Develop, review, enhance, and update all security-related policies and guidelines such as data classification, access control policies, data protection policies, staff security training policies, segregation of duties, data disposal and retention, password criteria, timeout requirements, user rights, etc.
  - Responsible for disaster recovery and business continuity planning and testing
- **Compliance, Audit, and Legal**
  - Understand, manage, and ensure compliance with legal, regulatory, and contractual requirements
  - Work closely with internal and external audit, privacy officer, and compliance officer
- **Leadership and Relationships**
  - Communicate about security and coordinate security activities with executive and technical leadership around the company
  - Work closely with leaders in HR and IT functional areas to ensure security standards, policies, and procedures are deeply embedded and understood
  - Lead security-focused culture and process change through training and interaction with department leaders

Author: Allyson Vicars | January 2018