KIRBYPARTNERS

Securing Healthcare's Infrastructure:
A Strategic Guide to CISO Hiring

TABLE OF

Contents

Introduction	3
IT Security Needs Review	4
Essential CISO Skills	6
Crafting an Effective Job Description	7
Sample CISO Job Description	9
Attracting High Quality Leaders	11
CISO Interviewing Strategies	12
CISO Interview Questions	13
Selecting Your CISO	15
Sustaining Excellence	16
About Kirby Partners	17

01 Introduction

Healthcare cybersecurity has evolved far beyond protecting passwords and preventing viruses. With patient lives, sensitive data, and organizational reputation on the line, cybersecurity has become integral to every aspect of healthcare delivery.

The Chief Information Security Officer (CISO) stands at this critical intersection of patient care, technology, and risk management. No longer just a technical role, today's CISO must be a strategic leader who can:

- Build security programs that protect patients while enabling innovation
- Navigate an ever-shifting landscape of threats and regulations
- Translate complex risks into clear business decisions
- Unite clinical, technical, and executive teams around security priorities
- Foster a security-minded culture across all levels
- Show that security investments provide value, reduce risk, and align with business objectives

Finding this caliber of leader requires a thoughtful, strategic approach. Whether you're hiring your first CISO or elevating your security program to the next level, the insights in this guide will help you build a resilient security foundation that advances your mission of delivering exceptional patient care.

02 IT Security Needs Review

Before writing a job description or starting your CISO search, conduct a thorough assessment of your organization's security landscape. This structured evaluation will help you define the scope of responsibility and required expertise for your new leader.

Include representatives from key stakeholder groups:

- Executive leadership
- IT and security teams
- Clinical operations leaders
- Risk management and compliance
- Privacy officers
- Department heads

Strategic Assessment Areas

Program Alignment

- Map security strategy to organizational goals
- Align with regulatory requirements (HIPAA, HITECH, etc.)
- Evaluate digital transformation security needs
- Define success metrics and KPIs
- Assess cybersecurity investment requirements
- Review current resource allocation

Technical Infrastructure

- Analyze current security architecture and controls
- Evaluate cloud security maturity
- Assess Zero Trust implementation progress
- Review security automation capabilities
- Document technical debt impact
- Evaluate security tool integration
- Review network security architecture

Medical Device Security

- Review medical device security protocols
- Assess vulnerability management processes
- Evaluate monitoring and incident response
- Document device inventory and risk levels
- Review IoT security controls
- Assess biomedical device integration

Compliance and Risk Management

- Analyze gaps in regulatory compliance
- Review risk assessment methodologies
- Evaluate incident response procedures
- Assess business continuity planning
- Review third-party risk management
- Document compliance remediation needs

Team Capabilities

- Document team structure and capabilities
- Identify security expertise gaps
- Assess security awareness effectiveness
- Review training requirements
- Evaluate the need for external support
- Review security culture maturity

Next Steps

1. Document all findings and key insights
2. Prioritize immediate vs. long-term needs
3. Use findings to shape your job responsibilities and qualifications
4. Create evaluation criteria for candidates

03 Essential Skills for Healthcare CISOs

A healthcare CISO requires expertise across three core domains, along with awareness of emerging technologies.

Technical Leadership

- Security architecture that supports clinical workflows
- Medical device and IoT security expertise
- Telehealth platform protection
- Emergency access protocols that don't compromise security
- Clinical-friendly security policies

Business & Operational Acumen

- Risk translation into healthcare business context
- Security alignment with patient care goals
- Budget management within healthcare reimbursement systems
- Navigation of healthcare regulatory requirements
- Metrics development for healthcare operations

Strategic Vision

- Security frameworks that enable digital transformation
- Scalable programs that adapt to healthcare changes
- Strong clinical and technical team partnerships
- Forward-thinking security architecture

Emerging Technologies

- Utilizing AI and machine learning for threat detection
- Preparing for quantum-resilient encryption
- Addressing zero-day vulnerability management
- Implementing automation in incident response

04 Crafting an Effective CISO Job Description

Transform your security needs assessment into a compelling job description that attracts top healthcare security talent.

Strategic Components

Position Summary

- Lead with patient care impact and healthcare mission
- Define reporting relationships and team size
- Connect security strategy to clinical operations
- Highlight digital transformation leadership
- State organizational size and complexity

Key Responsibilities

Organize into functional areas:

Strategic Leadership

- Board and executive engagement
- Program development and governance
- Budget and resource management
- Stakeholder relationship building
- Vision and roadmap development

Security Operations

- Clinical systems protection
- Medical device security
- Incident response leadership
- Security architecture design
- Technology implementation

Risk & Compliance

- Healthcare regulatory compliance
- Security policy development
- Third-party risk management
- Privacy program alignment
- Audit and assessment oversight

Innovation & Transformation

- Digital health initiatives
- Cloud security strategy
- AI/ML implementation security
- Emerging technology evaluation
- Security automation initiatives

Qualifications

Education

- Define minimum degree requirements
- Specify preferred advanced degrees
- List continuing education expectations

Experience

- Set years of security leadership required
- Specify healthcare industry experience
- Define budget management scope
- Detail team leadership requirements
- Outline technical expertise needed

Certifications

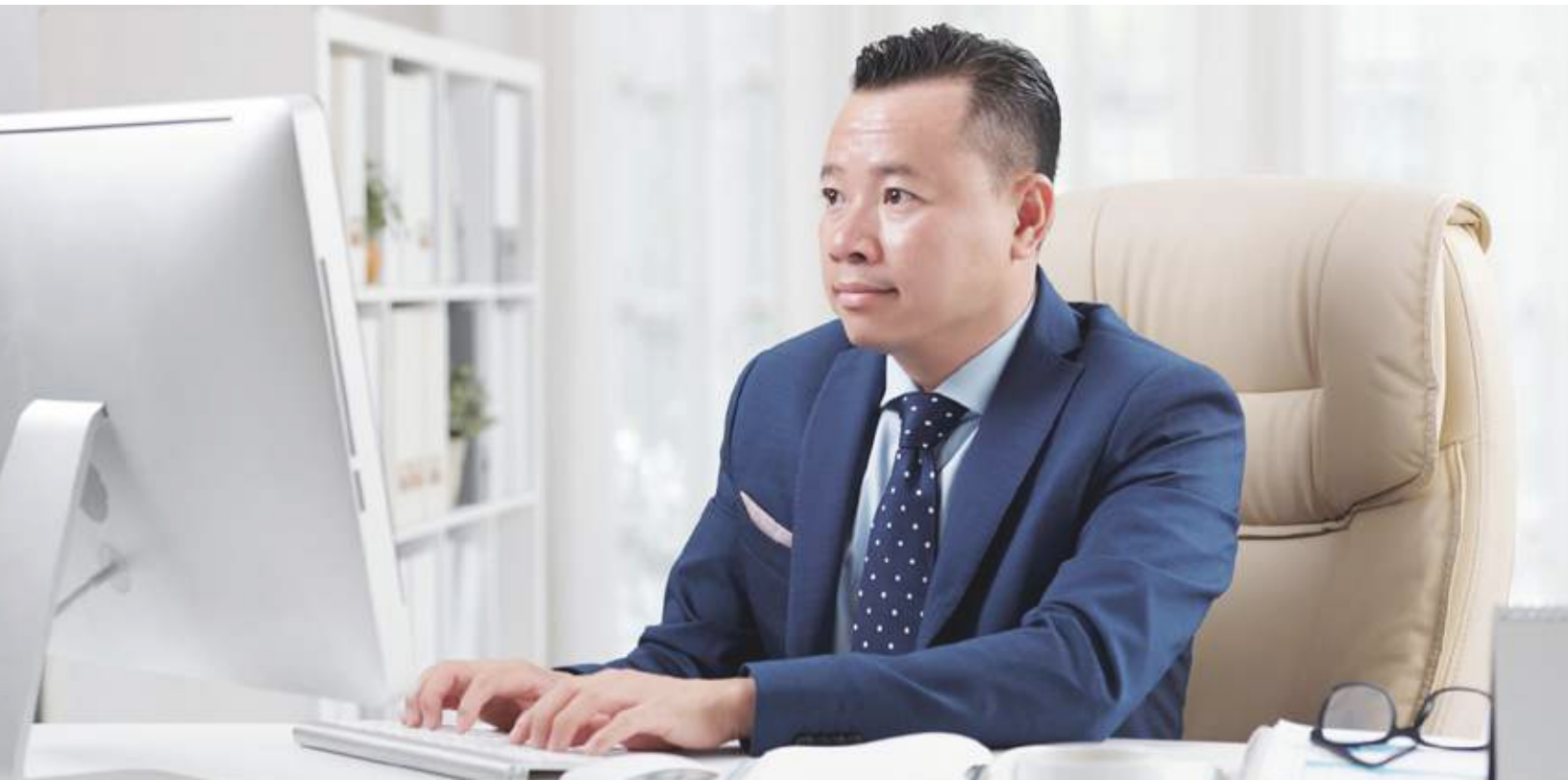
- List required certifications (e.g., CISSP)
- Identify preferred healthcare certifications
- Specify ongoing certification requirements

Writing Guidelines

- Use clear, action-oriented language
- Include specific metrics where possible
- Balance technical and leadership requirements
- Highlight growth opportunities
- Define work arrangements

Goals

- Accurately represents role and expectations
- Attracts top healthcare security leaders
- Aligns with market standards
- Differentiates your opportunity
- Appeals to diverse, qualified candidates



05 Sample CISO Job Description

Organization Overview

XYZ Health is a leading integrated healthcare system serving more than 2 million patients annually across three states. With 12 hospitals, over 200 outpatient facilities, and a nationally recognized telehealth program, we are committed to delivering high-quality, patient-centered care. Our focus on digital transformation and cybersecurity has earned us HIMSS Stage 7 recognition and a spot among *Newsweek's* "Most Wired" hospitals. As we continue to advance our technology and security posture, we are seeking a strategic and forward-thinking Chief Information Security Officer (CISO) to lead our enterprise-wide cybersecurity initiatives, safeguard patient data, and ensure the resilience of our digital infrastructure.

Position Summary

Reporting to the SVP/CIO, the Chief Information Security Officer (CISO) will lead our enterprise security strategy while enabling innovative healthcare delivery. This executive will build and maintain a comprehensive security program that protects patient data, clinical systems, and organizational assets while supporting our mission of exceptional patient care.

Key Responsibilities

Strategic Leadership

- Drive enterprise security vision aligned with healthcare innovation goals
- Lead development and execution of multi-year security roadmap
- Manage a multi-million dollar security budget
- Build and mentor high-performing security teams
- Partner with clinical, IT, and business leaders on digital transformation
- Present security strategy and metrics to Board and executive teams

Security Operations

- Design security architecture that supports clinical workflows and interoperability across enterprise systems
- Protect critical clinical systems and patient data
- Secure telehealth and remote care platforms
- Implement medical device security controls
- Lead incident response and business continuity programs
- Manage security operations center

Risk & Compliance

- Ensure compliance with HIPAA, HITECH, and industry regulations
- Direct security risk assessment and management program
- Oversee third-party risk management and vendor security
- Lead security audit and compliance initiatives
- Manage security policy development and governance
- Direct threat intelligence and vulnerability management

Innovation & Transformation

- Enable secure adoption of emerging healthcare technologies
- Guide security strategy for cloud transformation
- Advance zero-trust security principles across clinical and enterprise environments
- Direct security automation and orchestration initiatives
- Develop security governance for AI/ML applications in clinical and operational settings
- Lead enterprise-wide security awareness programs

Qualifications

Education

- Bachelor's degree required
- Master's degree in Information Security, Computer Science, or related field preferred

Experience & Expertise

- 10+ years dedicated IT security experience
- Proven experience managing multi-million-dollar security budgets
- Experience managing complex security incidents and regulatory interactions
- Board and executive committee presentation experience
- Expertise in cloud security architecture
- Strong knowledge of healthcare security and compliance frameworks
- Experience managing security in hybrid/remote environments
- Technical expertise in security protocols and emerging issues
- Track record of developing and retaining security talent

Certifications

- CISSP or CISM required
- HCISPP, HITRUST CCSFP, or CHPS preferred

Work Arrangements

- Hybrid role with minimum of three days per week on-site
- Up to 25% travel for multi-site security, vendor assessments, and events
- 24/7 availability for critical security incidents

06 Attracting High-Quality Leaders

Here are strategies to make your organization stand out and appeal to highly accomplished candidates:

Showcase Your Organization's Commitment to Cybersecurity

- Highlight digital health initiatives and innovation programs
- Showcase board-level support for cybersecurity
- Emphasize investment in security technologies
- Share success stories of security program impact

Offer Competitive Compensation

- Research current healthcare CISO compensation trends
- Consider regional market variations
- Structure packages including:
  - Salary benchmarked to market
  - Performance bonuses
  - Long-term incentives
  - Executive benefits
  - Professional development funds
  - Industry conference budgets

Emphasize Growth Opportunities

- Outline potential career progression paths within the organization.
- Highlight opportunities to lead innovative projects or initiatives
- Showcase how the CISO role contributes to overall organizational strategy
- Demonstrate commitment to security team leadership development

Promote Work-Life Balance and Organizational Culture

- Emphasize your organization's mission and values
- Highlight flexible work arrangements, if available
- Showcase your organization's commitment to employee well-being

Optimize Candidates' Experience

- Streamline the application process with a user-friendly, mobile-responsive system
- Maintain clear and consistent communication throughout the recruitment journey
- Provide prompt feedback after each stage of the interview process
- Offer personalized interactions with key stakeholders and potential team members

Learn more about candidate experience best practices in Kirby Partners' "The Route to Delivering an Exceptional Candidate Experience"

07 CISO Interviewing Strategies

Applying best practices on this page will help your organization assess candidates thoroughly and make informed hiring decisions.

Streamlining the Interview Process

Moving candidates quickly through the interview process reduces the chance they'll accept a competing offer while demonstrating that you value their time and are serious about their candidacy.

- Establish a compressed timeline for the entire interview process and communicate this to candidates upfront
- Pre-arrange stakeholder availability to avoid delays in scheduling interviews
- Leverage video interviews for initial rounds
- Reduce the number of separate interview sessions; consider panel interviews or full-day events where candidates meet multiple stakeholders
- Offer quick feedback after each interview stage to keep candidates engaged and informed
- Empower your hiring team to make quick decisions when they encounter exceptional candidates

Preparing for Interviews

Brief stakeholders on the role requirements and provide them with relevant questions to ask during their interactions with the candidate. To support a streamlined process, consider organizing a single day of back-to-back interviews with all key stakeholders. This approach respects the candidate's time and allows for a comprehensive evaluation in a condensed timeframe.

- Review the candidate's resume and application materials thoroughly
- Familiarize yourself with the job description and key requirements
- Prepare a structured interview guide with specific questions
- Involve key stakeholders in the interview process and brief them on their roles

08 CISO Interview Questions

The following list offers a sample of key questions for CISO candidates. These represent some of the most revealing questions from our comprehensive list. Select the questions that best align with your organization's needs, challenges, and culture.

Opening / Rapport-Building Questions

1. Please give a two-minute overview of your career, focusing on your cybersecurity responsibilities.
2. What interests you about the CISO opportunity?
3. What attracted you to healthcare security versus other industries?
4. What is a significant goal or initiative you pursue outside of your professional responsibilities?

Leadership and Cultural Fit

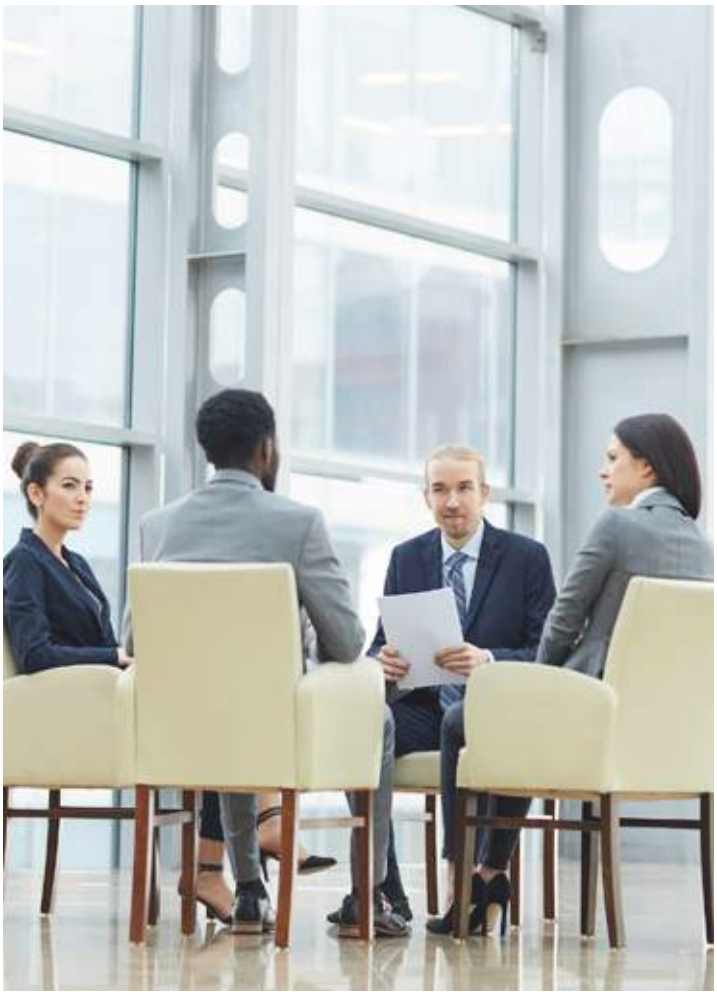
1. Please tell us about your approach to building high-performing teams and leading them through change initiatives.
2. How do you balance security and innovation in developing a security program?
3. Describe your experience presenting to and advising boards of directors on cybersecurity matters.
4. How do you ensure security maintains a service-oriented approach while protecting the organization?
5. How have you handled situations where you needed to influence decisions outside your direct authority?
6. What has been your experience managing remote security teams?
7. What strategies do you use for recruiting and retaining security talent?
8. How do you approach succession planning and developing future security leaders?

Healthcare Security Expertise

1. How do you balance security controls with clinical workflow efficiency?
2. What experience do you have securing telehealth platforms?
3. How do you approach medical device security governance?
4. Can you describe your experience developing security controls for Epic and EHR systems?
5. What strategies have you used to secure connected medical devices and IoT in clinical settings?
6. How do you approach securing AI/ML technologies in healthcare applications?
7. What healthcare security working groups or information sharing communities have you participated in?

Technical Leadership

1. How would you structure and implement a security governance program?
2. What security frameworks have you implemented in healthcare settings?
3. How do you integrate privacy regulations into security programs?
4. What is your approach to cloud security in healthcare?
5. How do you leverage security automation while maintaining proper oversight?
6. Describe your experience leading large-scale cloud migrations.
7. What's your approach to security tool consolidation and optimization?



Supply Chain & Vendor Management

1. How do you approach managing complex vendor ecosystems?
2. What's your methodology for software supply chain risk management?
3. How do you assess and monitor third-party security risks?
4. What frameworks do you use for vendor security assessments?

Crisis Management

1. Describe your experience managing teams during transformation or crisis.
2. Walk us through your process for handling large-scale security incidents.
3. What has been your approach to developing and testing business continuity plans?
4. How would you address a critical security breach caused by a third-party vendor?

Demonstrated Experience

1. Tell us about a significant security incident you managed and lessons learned.
2. Describe a time when you balanced protecting patient data with ensuring uninterrupted care.
3. Share an example of building or significantly enhancing a security program.
4. Describe a situation where budget constraints forced tough prioritization decisions.

09 Selecting Your CISO

After interviews conclude, gather feedback promptly from all participants.

Within 48 hours, convene to discuss impressions and evaluate candidates against predetermined criteria. Consider how well each candidate's vision aligns with your organization's security and compliance requirements, and assess any potential red flags in their approach to risk management and data protection.

When making your final decision, weigh both technical cybersecurity expertise and cultural fit. Evaluate each candidate's understanding of healthcare security frameworks and their ability to lead security initiatives while balancing clinical operations'needs.

Pay close attention to how effectively they communicated their security strategy and incident response plans.

Look for candidates who can articulate a clear vision for security program maturity while also showing the leadership qualities necessary to build relationships across clinical, IT, and administrative departments. This balance of skills is crucial for maintaining robust security controls while supporting healthcare delivery and patient care objectives.

Once you've made your choice, act decisively. Reach out to the selected candidate promptly with an offer, prepared to negotiate terms swiftly to secure their commitment. Remember that experienced healthcare security leaders are in high demand in today's threat landscape.

10 Sustaining Excellence in IT Security

The journey doesn't end with hiring the right leader. The technology landscape is constantly evolving, and to ensure your CISO can lead effectively into the future, consider these key strategies:

Continuous Learning

- Encourage ongoing education and professional development. The rapid pace of technological change demands that IT security leaders stay abreast of emerging AI and machine learning trends for advanced threat detection trends and adopt best practices.

Industry Engagement

- Support participation in industry conferences and professional organizations like CHIME and The Scottsdale Institute. These platforms offer valuable opportunities for knowledge exchange and networking.

Flexibility

- Build flexibility into the role to adapt to changing healthcare and technology trends. The ability to pivot strategies and embrace new technologies will be crucial for long-term success.

Innovation Culture

- Foster a culture of innovation that embraces new ideas and AI technologies. Encourage your IT leadership to create an environment where creative problem-solving and calculated risk-taking are valued.

Succession Planning

- Develop a succession plan to ensure continuity of IT security leadership. This safeguards your organization against unexpected transitions and provides a pathway for nurturing future leaders.

11 About Kirby Partners

Specialized Leaders, Superior Results

We find future-ready leaders to fill your critical C-suite, VP and director roles.

Our expertise:

- Chief AI Officers
- Chief Data Officers
- Chief Digital Officers
- Chief Digital and Information Officers
- Chief Executive Officers
- Chief Human Resource Officers
- Chief Information Security Officers
- Chief Information Officers
- Chief Innovation Officers
- Chief Medical Information Officers
- Chief Privacy Officers
- Chief Research Information Officer
- Chief Risk Officers
- Chief Technology Officers
- VPs/Directors of Application, Security, and Technology
- VPs & Directors of HR
- Enterprise Architects

Kirby Partners' completed executive searches

Unrivaled Experience and Connections

We excel at finding leaders who make transformative contributions and stay committed for the long term.

- 36 years of retained executive search experience
- Recognized as one of *Modern Healthcare's* "Largest Executive Search Firms"
- Named to *Forbes'* list of "America's Best Executive Search Firms"
- Certified woman-owned business committed to fostering diversity
- 100+ successful senior leadership searches in the last five years

To learn more about Kirby Partners, schedule a discovery call with our team.

Judy Kirby, CEO
jkirby@kirbypartners.com
kirbypartners.com
407.788.7301