The Ultimate CISO Job Description

Chief Information Security Officer

a.k.a.

Chief Security Officer (CSO)
Vice President, Director or Head of
Information Security or Cybersecurity

By

Heller Search Associates

Introduction

It should come as no surprise to any business professional that securing data and information assets has become a top priority for virtually all companies and institutions. Hardly a week goes by without news of yet another major security breach, or the revelation of the theft of reams of confidential customer data.

Companies impacted by security breaches are finding that these incidents damage their brands and cause angry customers to take their business elsewhere. As a result, information security has become a board level concern.

These conditions are focusing the spotlight on the Chief Information Security Officer (CISO) role at most companies. Now more than ever, the CISO function is one that companies cannot afford to get wrong

The Expanded CISO Remit

The Heller Search team is recruiting an increasing number of CISO positions for our clients. We have seen first-hand that companies need a senior executive who, in addition to assuming full responsibility for securing the enterprise, can communicate security concepts and strategies in business terms, and raise the board of directors' understanding of security beyond a 'compliance-only' view.

In addition to deep experience and technical knowledge in the security domain, companies are seeking a business professional who understands the concepts around risk, and who possesses the communications and influencing skills to evangelize new security policies and drive adoption in every corner of the organization.

Why Have We Created *The Ultimate CISO Job Description*?

The executive search team at Heller Search has created this resource to help CIOs, CEOs and their HR and talent acquisition partners produce a profile of a CISO who possesses the technical, leadership and communications skills to lead information security today. It is our hope that this resource will help you define and attract the best and brightest information security executives available in today's talent market.

To use this as a template to write your CISO job description, click here to download the MS Word version of this document, ready for your edits.

Table of Contents

Summary of sections in this document

(Click to jump to a section)

Conventions used in this document:

- ✔ A suggestion that applies to most CISO positions.
- ☐ In consultation with the hiring committee and your external recruiting partner, consider whether this suggestion applies to your CISO position. Delete those that do not apply.
- ✔ _____ Add to the list here, based on specifics of your company, your culture and the goals of the business.

I. POSITION TITLE

The complete title for the position being recruited. For example:
Vice President and Chief Information Security Officer (CISO), [Company]

II. ABOUT THE COMPANY

Provide a brief overview of the company, and a website link. Boilerplate copy from your website or a press release may offer a good start, but you may wish to edit this language to suit your target audience of potential CISO candidates.

Suggested contents for this section:

- ✔ **Full name of the company**
- ✔ **Headquarters physical address**
- ☐ **Primary locations**
- ✔ **Company logo**
- ✔ **Website address**
- ✔ **Company description**
- ☐ **Mission or values statement**
- ☐ **Notable brands and major milestones**

- [x] Annual revenues or a comparable metric
- [ ] Total employees

III. ABOUT THE HIRING MANAGER

In this section, provide a short introduction to the executive that your CISO will report to. Suggested contents for this section:

- [x] Name
- [x] Full job title
- [x] Year they joined the company
- [ ] If promoted, their previous roles at the company
- [x] Notable roles before joining the company
- [x] Brief professional bio
- [ ] Headshot photograph

IV. POSITION SUMMARY

This section is the elevator pitch, or the executive summary of the CISO role that by itself provides readers with a basic understanding of the type of information security professional you seek. This should be a relatively short summary, as later sections will provide all of the detail. For example:

[Company] is conducting a search for an experienced and highly qualified Chief Information Security Officer (CISO). The CISO is responsible for establishing and maintaining the enterprise vision, strategy, architecture, and a multi-year roadmap that ensures that the company's information assets are adequately protected.

A key element of this role is communicating security at a strategic level to executive management, the Audit and Compliance Board, and the Board of Directors and evangelizing security across the business to drive adoption of security best practices.

The CISO will manage a small team of dedicated resources and a larger team of matrixed resources.

V. KEY RESPONSIBILITIES

In this section, list the major areas for which the CISO will be accountable.

- ✔ Develop and implement a strategic, long-term information security strategy and roadmap to ensure that [Company]'s information assets are adequately protected.
- ✔ Work with senior leaders across the business to assess and communicate acceptable levels of risk.
- ✔ Identify, evaluate and report on information security risks, practices and projects to the Executive Committee and the Board of Directors, and provide subject matter expertise on security standards and best practices (e.g. FFIEC, Dodd-Frank, SOX, PCI, etc.).
- ✔ Develop, mentor, and manage a high performing staff of information security professionals.
- ☐ Chair the information security steering committee (or governance board, or advisory board).
- ☐ Develop the Board's understanding of security beyond a 'compliance-only' view.
- ✔ Lead the development of up-to-date information security policies, procedures, standards and guidelines, and oversee their approval, dissemination, and maintenance.
- ✔ Ensure that the security management program is in compliance with applicable laws, regulations, and contractual requirements.
- ✔ Act as the champion for the enterprise information security program and foster a security-aware culture.
- ✔ Oversee the evaluation, selection and implementation of information security solutions that are innovative, cost-effective, and minimally disruptive.
- ✔ Partner with enterprise architects, infrastructure, and applications teams to ensure that technologies are developed and maintained according to security policies and guidelines.
- ✔ Manage regular intrusion detection and vulnerability reporting, internal and external IT audit groups reviews, and the coordination of all required fixes.
- ✔ Develop business metrics to measure the effectiveness of the security management program, and increase the maturity of the program over time.

- ✔ Monitor the industry and external environment for emerging threats and advise relevant stakeholders on appropriate courses of action.
- ✔ Liaise with law enforcement and other advisory bodies as necessary to ensure that the organization maintains a strong security posture.
- ☐ Oversee incident response planning and the investigation of security breaches, and assist with any associated disciplinary, public relations and legal matters.
- ✔ Oversee and lead the creation, communication and implementation of a process for managing vendor risk and other third party risk.
- ✔ Lead due diligence and post integration activities related to information security for all M&A activity.
- ✔ _____
- ✔ _____

VI. QUALIFICATIONS

In this section, list the career experience, educational background and technical skills and certifications necessary for a candidate to succeed in the CISO role.

- ✔ Bachelor's Degree in computer science, engineering, or a related field; (graduate degree preferred).
- ✔ Minimum 10 years of IT and/or business leadership experience, and 5+ years of information security/cybersecurity experience.
- ✔ A proven track record in developing information security policies and procedures, and successful execution.
- ✔ Extensive knowledge of business risk, risk assessment and risk-based decision making.
- ✔ Able to communicate security and risk-related concepts to both technical and non-technical audiences (in business terms), including board level.
- ✔ A natural influencer and coalition builder; passionate about building high performing teams.
- ✔ Ability to inspire and motivate cross-functional, interdisciplinary teams to achieve tactical and strategic goals; an innovative leader, problem solver and consultant.

- [x] Ability to evangelize IT security to make it a critical part of business operations; build trust and respect for the security function.
- [x] Excellent written and verbal communication, interpersonal and collaborative skills.
- [x] Experienced with contract and vendor negotiations.
- [x] Ability to effectively prioritize and execute tasks in high-pressure situations.
- [ ] Knowledge of security, risk and control frameworks and standards such as ISO 27001 and 27002, SANS-CAG, NIST, FISMA, COBIT, COSO and ITIL.
- [x] Understanding of cloud, SaaS, and IoT architectures, and their implications on information security strategy.
- [ ] Technical acumen including but not limited to: OSI, IT infrastructure, cloud, application development languages, tools and frameworks, database technologies, web technologies, next gen mobile, network architecture, enterprise architecture, and directory services.
- [ ] Security technology acumen and experience including but not limited to: firewall, intrusion detection, cyber-attack tools and defenses, encryption, certificate authority, web filtering, anti-malware, anti-phishing, identity and access management, multi factor authentication.
- [ ] Professional certifications, such as a CISSP, CISM, CISA.
- [x] _____
- [x] _____

VII. LOCATION AND TRAVEL REQUIREMENTS

The city where will the CISO be located and a short description of the amount and nature of business travel. For example:

> The CISO will work from [Company] headquarters in [city], [state] and is expected to travel approximately ____ percent of the time, mostly to our U.S. locations. (with international travel expected approximately ____ times per year).

VIII. WHY THIS OPPORTUNITY IS COMPELLING

This is your opportunity to sell the company and the CISO job to potential candidates. Ask yourself: Why would a strong information security leader, who most likely already has a great job, or competing offers, consider joining your company? What would you tell her about the position, the company and your culture to pique her interest? For example:

The CISO at [Company] will

- ✔ **Establish a world-class information security capability at a growing company that is a leader in its field.**
- ✔ **Be a member of a successful and forward-looking IT leadership team.**
- ☐ **Lead in a high-profile role that interacts regularly with the board.**
- ✔ **Join a culture of collegiality and respect [or insert 2-3 company values].**
- ☐ **(Build and) Lead a high performing team of information security professionals.**
- ☐ **Make a significant difference through exceptional information security for the enterprise.**
- ☐ **Join a forward-thinking team of leaders who work together toward a common goal.**
- ✔ _____
- ✔ _____

IX. INTERVIEW PROCESS

Provide interested candidates with a high level summary of the major stages in the interviewing and hiring process.

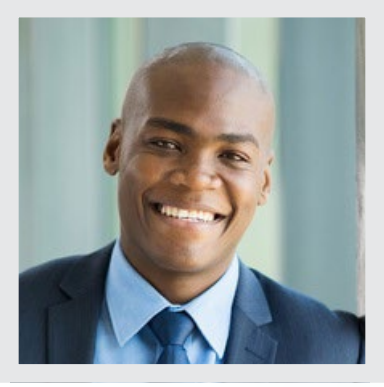
- ☐ **First interview with HR representative [or executive search partner]**
- ☐ **Candidate presentation to the hiring committee by [executive search partner].**
- ✔ **Initial interview by phone.**

- [x] First round of interviews at [Company].
- [x] Second round of interviews.
- [x] Background and reference checks.
- [x] _____
- [x] Offer and acceptance
- [ ] Drug screen
- [x] Start

X. CONTACT INFORMATION

Provide the contact details for the person or people on the hiring committee, or at your executive search partner, whom interested candidates can get in touch with to learn more about the position, and submit their resumes. For example:

Qualified candidates should contact:



- [x] Name
- [x] Job title
- [x] Company (may be name of executive search partner firm)
- [x] E-mail address
- [x] Office telephone number
- [ ] Cell phone number
- [ ] Headshot photograph

XI. ADDITIONAL RESOURCES

- Download an MS Word version of this CISO job description ready for your edits
- 26 Cybersecurity Acronyms and Terms IT Recruiters Should Know
- Wikipedia's Chief Information Security Officer page
- Download the Ultimate CIO Job Description

XII. ABOUT THE AUTHORS

This Ultimate CISO Job Description was written by the members of the executive search team at Heller Search Associates:

Martha Heller
Founder & CEO

Carol Lynn Thistle
Managing Director

Kelly Doyle
Managing Director

Steve Rovniak
Executive Director

Pamela Kurko
Recruiting Partner

Katie Ross
Recruiting Partner

Brittany Jeeves
Associate Recruiter

Lauren O'Connor
Operations Manager

Feedback Welcome

We'd love your feedback, including suggested additions or edits to this resource.

Send us your comments!

About Heller Search Associates

Heller Search is a retained executive search firm specializing in Chief Information Officers (CIO), Chief Technology Officers (CTO), Chief Information Security Officers (CISO) and all senior information technology positions (VPs and Directors of IT) nationwide, in all industries. Our clients include Fortune 500 as well as mid-market companies, higher education, non-profits, small businesses and high tech startups. Heller Search is a Certified Women-Owned Business Enterprise.

Heller Search Associates, Inc.
33 Lyman Street
Westborough, MA 01581

(508) 366-7005

www.hellersearch.com