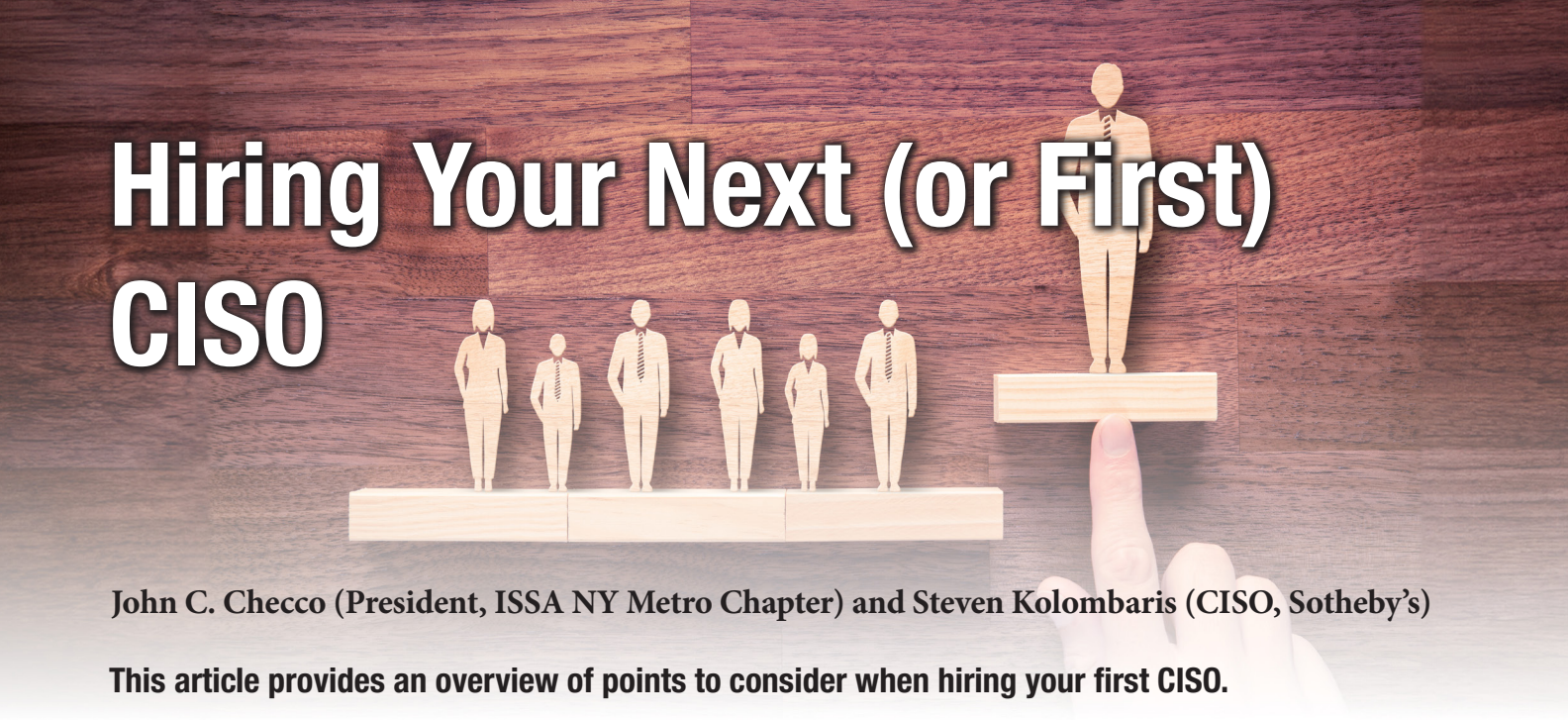
Hiring Your Next (or First) CISO



John C. Checco (President, ISSA NY Metro Chapter) and Steven Kolombaris (CISO, Sotheby's)

This article provides an overview of points to consider when hiring your first CISO.

You are a growing company, and your board (or regulations such as NYS DFS 500) requires you to hire your first CISO. Heed this business management cliché: "Failing to spend time now to do it right will cost you time to do it twice."

A peer who has been a CISO in multiple industries offers the analogy of a landowner who wants a house, so they hire a general contractor. They realize the general contractor is there to achieve that goal by applying knowledge, experience, expertise, capabilities, connections, tools, in-house and external resources. Yet, many organizations hire a CISO without examining either their goals or the CISO's skills but expect to be handed immediately a "Cybersecurity Level Achieved" badge.

CISOs are the general contractors for cybersecurity. They work to achieve an organization's security goals through their own knowledge, experience, expertise, capabilities, connections, tools, in-house and external resources.

Here are our suggestions for doing it right the first time.

Define the CISO Role

Writing and broadly disseminating a job requisition is not your first step. Too often, the job description for the CISO position is left to HR, an external recruiting agency, or written internally by the CTO or other technology-focused executive. This leads to job descriptions that vary wildly from governance, to hands-on firewall maintenance, or reflects a buffet of skills that no one person possesses.

The correct first steps are analysis, comprehension, and reconciliation of the following factors:

1. Board and/or executive committee ask;
2. Regulatory minimum requirements;
3. Needs of the organization;
4. Responsibilities for the CISO;
5. Where the CISO best fits into the reporting structure; and
6. Justifying a compensation package.

Once these six items have been properly vetted and documented, you can work with the executive committee to build the right level of language for the job requisition.

Deconstructing the Board Ask

Although it seems forward-thinking that the board has requested the creation of a CISO role, deeper exploration of the 'ask' is truly needed.

- What factors brought about this request?
  - Internal incident, direct or indirect (with suppliers/partners);
  - Internal risk report;
  - External event or industry tailwind; or
  - Regulatory compliance, recent audits or other examinations.
- What is the board really asking for?
  - Additional business risk governance;
  - Explicit security program; or
  - Other objectives (or checkbox confirmation).
- What is the board expecting to see delivered?
  - Position fulfillment;
  - Regular risk (and risk exception) reporting; or
  - Explicit security initiatives.
- What is the expected reaction if the CISO challenged the board?
  - Board is expecting to be challenged;
  - Board is expecting confirmation, not challenge (narcissism); or
  - Board's security governance committee will work with the CISO through challenges.

Determining Regulatory Scope

Another aspect of the CISO role is the scope of regulatory requirements the organization must comply with regarding information security and data privacy. It is also important to note that regulatory compliance does not make a security program successful.

If your company is a service organization or removed from direct regulatory requirements, understand the impact from your clients' regulatory obligations and align your company's scope using standards such as ISO-2700x and/or SOC2 compliance.

There is a dichotomy where CISOs view that compliance is far below the minimum standard for security, whereas organizations view regulatory compliance as their maximum spend. Deciding what level of control beyond compliance can be afforded to the CISO position is a crucial factor in determining the job's responsibilities.

Organizational Security Roadmap

By the time an organization has decided to engage its first CISO, there may have been an incident or event that triggered this need. This implies that the organization has already gained some realization of its existing security posture.

In developing the CISO role, one must identify and document the status quo, and determine an ideal target state. Given those two endpoints (and assuming your organization could never fully reach this ideal target), the hiring manager should plan alternative paths and first steps needed to bolster the security program.

These paths and steps will define the first two years of the CISO role. Beyond that, we can expect both organizational and environmental changes to mold the CISO role perhaps in a different direction. However, understanding these paths will help vet candidates who understand the roadmap.

Responsibilities of the CISO

Given the detailed nuances of the ask, minimum and maximum requirements (also known as guardrails), and the tentative security roadmap, the hiring manager can define the high-level responsibilities for the newly created CISO position. These can be further broken down into four main buckets:

Governance, Risk and Compliance (GRC)

GRC is the administrative branch of the security team that manages policies and their supporting controls, audits, upward (board) reporting, and maintaining the aggregate risk register.

Security Operations (SecOps)

The Security Operations Team employs security technologies to support the controls, monitor users and networks for anomalous activities, investigates events, and mitigates incidents.

Security Technologies

The Security Technologies Team, which may or may not report to the CISO or CTO, deploys and maintains the tools needed for the other branches to operate effectively.

Business Unit Risk Management (BISO)

The BISO team works with each business unit to assess risks in both operations and development help prioritize security issues with their operational issues, define roadmaps for reducing risk exceptions, work with business leaders to gain budgets for security initiatives, and report on the overall security health of the business unit.

Sanity Check #1: Structuring Exercises

If these structuring exercises–pertaining to scope, roadmap, and responsibilities–do not resonate with your organization, perhaps the role they seek is not that of a CISO. Many times, the title of "*Information Security Officer*" is misused hoping to attract more candidates; but in reality, the organization is looking for skills associated with a *Security Analyst or Policy Manager.*

Aligning the CISO in the organization's structure for success

Defining the material responsibilities of the CISO also means understanding where in the organizational reporting chain those responsibilities will be most successful. Todd Inskeep has analyzed the benefits for each reporting option:

REPORTING	RATIONALE	BENEFITS
CIO	The CIO is responsible for managing and classifying the organization's information.	• Natural tie between security and information. • Peer relationship with CDO (Chief Data Officer)
CTO	The CTO handles the technology infrastructure and operations.	• CISOs get greater exposure to the operations. • Security tooling requires heavy support from the technology team.
CFO	Cyberattacks and data breaches measurably affect the bottom line.	• Provides a fiduciary voice at the leadership table. • CFO better understands the costs of risks.
CRO	Security is an enabler for reducing business risk.	• CRO is already a recognized leader and could help foster security agenda. • Moves security out of CIO/CTO technology-centric organizations, making it clear cyber risk is part of the broader risk management agenda.
GENERAL COUNSEL	GC and CISO have similar incentives to ensure policies enable the company to meet legal obligations.	• General Counsel supports security projects that have a governance/compliance component. • CISO gains exposure to other parts of organization.
CEO / BOARD	The company has a mature security program and security is core to the business.	• Demonstrates management's commitment to the strategic importance of the CISO's role. • Working closely with the CEO ensures alignment of security with strategic business objectives. • Provides CISO positional authority to drive a security agenda. • CISO is positioned equal to other (revenue-generating) parts of the business, increasing ability of prioritizing security in those areas.

REPORTING	RATIONALE	BENEFITS
BELOW C-LEVEL	CISO is an operational role, rather than an executive role.	• Ability to work closely with operational teams to get projects done without layers of overhead.

If the CISO will be the main communicator of incidents to the board, then subsuming them under any other CxO is counter-productive to their ability to enact change. For example, if your most important asset was rendered unusable, would the top-level CxO accept responsibility, or does it fall on the CISO to mitigate? If the audit/regulatory (or even client) confidence does not clearly involve the CISO in the planning stages but is required to deliver, can that CISO effectively manage without authority?

Positioning the CISO for success also means positioning the CISO for authority and responsibility. Unfortunately, many top-level CxOs may feel that giving the CISO equal share in leadership means diluting their own budgets and authorities; political fiefdoms are alive and well in many organizations.

Rightsizing the CISO compensation package

CISO–or any executive–compensation is based on both responsibilities and expertise required to execute those duties. As a hiring manager, do not fall into the falsehood of "aligning compensation with the market" or "restricting compensation based on internal senior management pay ranges." Although both factors play a key role in determining compensation, there are other issues that should allow a candidate to measure above the corporate-defined salary range:

- Experience in executing similar objectives in other industries;
- Demonstrable expertise in your organization's industry;
- Reputation of the candidate amongst their peers;
- Delivery of management business objectives (MBOs) based on knowledge; and
- Ability to lead culturally within the political realm of the organization.

In short, if your organization cannot compete financially, this may show a more systemic problem than cybersecurity.

Sanity Check #2: Positioning Exercises

If these positioning exercises–reporting chain and compensation–are not within your control, the role they seek is not that of a CISO but of a lower role such as security operations manager.

Job Requisition

At this point, one can document a robust job description. This first pass at documenting the role is extremely important but should be kept internally. The externally facing job description needs to be direct, clear, and concise. The elements of an attractive CISO job description include:

- Organization purpose for the position
- Primary responsibilities (abridged)
- Reporting structure (level and reporting purpose)
- Collaboration requirements (upward, downward, and lateral)
- Compensation factors (i.e., executive contract or employee salaried)

Executive Candidate Selection

Unlike other executive roles, the CISO needs to communicate complex concepts and issues tangibly to allow boards, business units, and operational teams to own cybersecurity and make educated decisions. As such, selecting CISO candidates is much more difficult, as AI-based recruiting filters focus on hard skills rather than leadership skills.

To get quality candidates, it is worth the cost to engage an executive search firm that specializes in placing CIOs/CDOs or CSOs/CISOs. Avoid agencies purporting to place technology-focused roles such as CTOs and those focused on sales or marketing.

Your priorities determine which qualities you want to see in the next leader, but other stakeholders in the hiring process may have their own goals. You are likely looking for someone who can cure certain deficits. The hiring manager (or committee) may look for the best skill sets. Fulfilling both these visions requires a balancing act. But by driving the process, you can exercise a greater influence on the final candidate selection.

Candidate Primary Qualities

The primary qualities to consider include:

- Leadership skills — leaders have an ability to listen and be responsive, as well as to inspire and motivate.
- Organizational skills — every organization has some level of politics that the leader needs to navigate and influence.
- Relevant knowledge and experience — the executive needs a certain level of technical prowess and industry background.
- Cultural fit — look for a leader who can either augment your culture or disrupt it, depending on what your organization needs.

Besides these top qualities, consider secondary ones, such as:

- Management skills to oversee projects and programs
- Administrative skills to develop and manage budgets
- Change-management skills to usher the organization through changes
- Outside knowledge and experience to be innovative

Interviewing Candidates

Traditional interview processes include a phased approach: recruiter, HR, hiring manager, and some team members.

For a role such as the CISO where they will interact across departments and teams, it behooves an organization to allow the candidate to interview with cross-functional leaders and even several board members. This will give a more realistic representation of how the candidate will interact at various levels and demonstrate if they can effectively speak the specific dialect needed for each area.

Diversity & Inclusion

Ensuring diversity equality is important, especially at the senior leadership levels. In a large population, such quotas are beneficial to ensure representation across different experiences; but a mandated quota in a small pool of executives may present challenges to the new CISO whose perceived selection criteria outweigh the true value they bring to the organization.

There is a fine balance between hiring a candidate because they are diverse versus hiring a candidate who happens to be diverse. How does one hire for diversity without the new hire feeling devalued because of diversity quotas? A panel titled "Educating Future Leaders" at the 2020 NCSA conference held in NYC at NASDAQ broached this very subject, providing a thoughtful and interesting approach. The quota need not be in the hiring, but in the candidate pool itself. When there are finalists of equivalent capabilities, hiring for diversity then becomes not only defendable, but hugely beneficial to the organization.

Sanity Check #3: Candidate Pool

If the initial candidate pool is too small (< 3), too broad, or lacks in diversity, it is a red flag for a problem in the job requisition or the resource channels being marketed to. It may be time to revisit and reevaluate the steps that define the role.

Leadership Onboarding

Like succession planning, there needs to be an explicit plan to jumpstart the new CISO. The best way to give the new CISO some traction is to help build the initial relationships both internally and externally. This means allowing the new CISO to absorb some of the hiring manager's political capital as their own.

Lean In: Internal Introductions

Introduce the new CISO to the executive staff and collaborate on an overarching objective for the first 90 days.

Assist in creating the new CISO's memo to the board, outlining the objectives and the associated expectations of each group/department/team to meet those objectives.

Co-create a welcome letter to all groups/teams/members, introducing the new CISO leadership and outlining the initial vision of the security program.

Outreach: External Relationship Introductions

Notify clients/customers of the new security leadership and help schedule strategic customer visits within the first 90 days.

Subsequently, encourage the CISO to meet with any critical partner/supplier leadership.

If the new CISO is coming in from another industry, try to have them meet with industry leadership.

The First 90-Days

Before hiring your first CISO, many security functions–whether or not they were viewed as such–were handled by other leaders, business units, or operational teams.

Assignment

It is in these first 90 days where a CISO needs to identify those security functions and categorize them as either "security governance," "security operations," or "security technologies." The CISO must then navigate what can/should be moved into the various security teams, and what can remain with the existing structure.

Assessment

At the conclusion of the first quarter, the new CISO should be able to:

- Engage an external audit and compare against the new CISO's internal assessment.
  - Ideally, the audit should be an annual recurrence to provide consistency in security posture long term.
- Report on existing security posture, key areas of inherent risk, a rolling risk register, and the impact of existing risk exceptions.
- Present a set of recommendations for reducing inherent risks and removing and/or mitigating risk exceptions.
- Garner congruence on what teams/units own each risk–as the security team cannot own a risk created by another team over which they have no control.

Sanity Check #4: The 90-day Review

The first months of assessing the new CISO hire allow the observation of several factors that signify a successful role:

1. Leadership Traction / Cultural Fit
2. Comprehension / Strategic Direction
3. Communication

Unlike traditional hiring, it is acceptable to dismiss a CISO who causes more destructive distraction than constructive disruption. Finding the right senior executive is not always easy when other parts of the organization do not understand cybersecurity. Every setback is an experience to build on, and you may find that parts of the role's responsibilities were not as important as originally expected, whereas other responsibilities bubble up in priority.

Summary

In hiring a CISO for your organization, do your homework to envision what the role would be in three to five years. Do they enhance the organization's resiliency? Do they follow a good decision-making process? Are they respected by the board? Do they work well cross-functionally? Are they sought for advice by business units and other business leaders? Are they part of the corporate family? Will they have a seat at the adult table or be relegated to the kids' table?

The answer to these questions will put you on the path to a successful hire.

About the Authors

John C. Checco

John C. Checco is the president of the ISSA New York Metro chapter. He previously led the financial services practice at Proofpoint and served as a security executive at several large financial institutions.

Follow, connect with, and read more from Checco at https://www.linkedin.com/in/xn--fci/

Steven Kolombaris

Kolombaris is an experienced CISO and Board Member dedicated to information security. A design thinker fostering talent and guiding startups, he is the CISO at Sotheby's. Prior executive roles includes Blue Origin, Bank of America, JP Morgan, and Apple. He is an NYU and Stevens Institute alum, with an executive MBA (PLD) from Harvard Business School.

Follow, connect with, and read more from Kolombaris at https://www.linkedin.com/in/steven-kolombaris.