fortium partners

The CEO's Guide to Hiring a CISO

The CEO’s Guide to Hiring a CISO

Table of Contents:

This guide demystifies the process of hiring a CISO and provides you with the insights needed to make an informed CISO hiring decision. Since Gartner predicts that 45 percent of organizations will experience attacks on their software supply chains by 2025, the CISO role has become pivotal for short-term survival and long-term success.

Part 1: Overview

Technology leadership is pivotal in driving organizations forward by strategically planning, implementing, and managing technology resources. It encompasses using technical knowledge, tools, systems, and processes to foster innovation, achieve organizational goals, and maintain a competitive edge in the marketplace.

Technology Leaders, often part of the executive team supporting the CEO, oversee the investment in and utilization of technology. This section explores the:

- Concept of technology leadership,
- Technology consumer and technology creator organization types,
- Technology leadership roles appropriate for each type of organization, and
- Key roles that comprise technology leadership, including the Chief Information Officer (CIO), Chief Technology Officer (CTO), and Chief Information Security Officer (CISO).

What is Technology Leadership?

Technology, in the context of technology leadership, refers to using technical knowledge, tools, systems, and processes to create, develop, and manage innovative solutions that drive an organization or industry forward. *Technology Leadership* is an executive role that encompasses the strategic planning, implementation, and management of technology resources (both human and financial) to achieve organizational goals, foster innovation, and maintain a competitive edge in the marketplace.

Technology Leadership, then, is a subcategory of executive leadership primarily concerned with an organization's investment in and use of technology to further an organization's goals. Whether that organization primarily buys and implements technology for its own use or is a technology company that primarily creates technology products and services for other organizations to use, both usually have technology leaders overseeing these functions. Often confused with the executive leadership *of a technology company* (e.g., the CEO of a software company), technology leadership in this context is most often part of the leadership team that supports the CEO and is a peer to other functional leaders (CFO, CMO, CHRO, GC, etc.).

The definition of technology leadership is further narrowed to those leaders responsible for leading technology and report organizationally to a non-technology leader (most often the CEO or Division President, etc., but can be a functional leader such as the CFO in smaller companies). This would generally exclude direct reports of a technology leader unless the role achieves such significance that it often has alternative (e.g., "dotted line") reporting to a non-technology leader, as is the case for the Chief Information Security Officer (CISO) who often has dual reporting relationships to a CIO/CTO and Legal, Internal Audit, or the Board of Directors. Also excluded would be consulting professionals whose clients are technology leaders and their organizations but themselves do not have authority and responsibility over the human and financial technology resources of those organizations.

What types of Organizations Engage Technology Leadership?

Technology use in organizations has become so ubiquitous that all types of organizations in all industries use Technology Leadership to effect the strategic planning, implementation, and management of technology resources (both human and financial) to achieve organizational goals, foster innovation, and maintain a competitive edge in the marketplace. However, to better understand technology leadership, all organizations using technology leadership can be assigned to one of two broad categories:

1. **Technology Consumer** - Those organizations that primarily *consume* technology to produce their revenue

2. **Technology Creator** - Those organizations that primarily *create* technology to produce their revenue

Technology Consumers heavily depend on Technology Creators for innovation and transformation - and spend the bulk of $4 trillion annually to compensate Technology Creators for all technology products and services (data centers, software, devices, services, communications). This is not to say that Technology Consumers don't, at times, create technology or that Technology Creators don't use technology created by others. But, as the categories suggest, the key differentiator is whether the primary source of revenue (e.g., greater than 50%) is derived from *selling technology to other organizations* or derived from selling other products and services (banking, auto, construction, etc.) that benefit from consuming technology created by others.

Defining the two broad categories of organizations that engage in technology leadership is useful in understanding the *roles* that comprise technology leadership.

What is a CISO?

The Chief Information Security Officer (CISO) is a senior technology executive focused exclusively on shaping an organization's governance, risk management, and compliance posture and strategy - including digital or cybersecurity. The CISO's team protects an organization's digital assets from cyber threats and responds to any and all cybersecurity incidents that arise. Further, the role extends beyond mere protection; it also encompasses comprehensive cybersecurity incident management across your technology environment.

While this serves as a baseline definition for a CISO, the CISO's role is at a crossroads because of:

- the acceleration of cybersecurity breaches,
- the increased usage of generative AI tools, and
- stricter cybersecurity rules that emphasize disclosure requirements*

*Source: ASIS International

This guide will help you navigate the ever-evolving role of CISOs so that you can make an informed decision about hiring a virtual, fractional, or full-time CISO.

What is a CISO's role within the C-Suite?

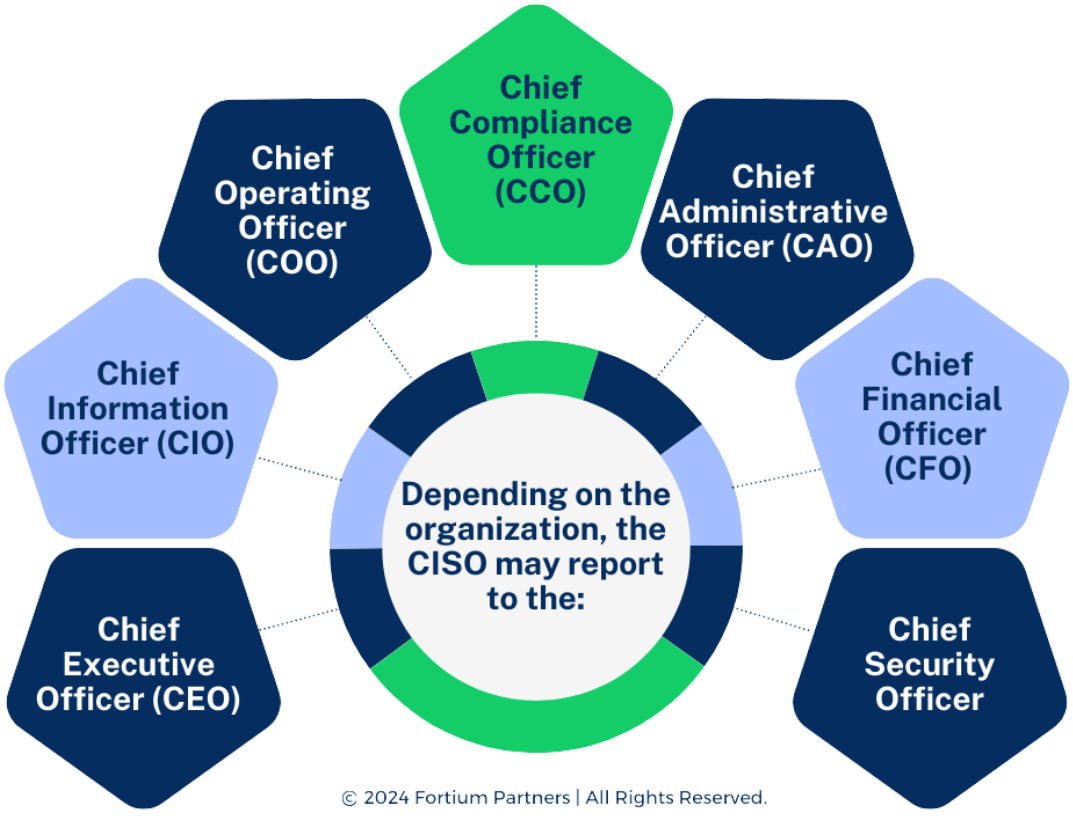
The CISO ensures that the C-suite clearly understands the cybersecurity posture of the organization. The CISO coordinates the C-level discussion regarding the strategic priorities of the Cybersecurity program. The CISO does this by providing visibility into the components of the Cybersecurity program. Visibility typically includes both the GRC (Governance, Risk, and Compliance) view focused on cyber risk and the operational technology, which encompasses the technical controls and programs mitigating cyber risk. However, some organizations may prefer to manage the operational technology aspects through a CIO who would work in concert with the CISO to implement the CISO's strategy that protects the cybersecurity posture of an organization. Furthermore, the CISO provides the methodology for cyber incident response plans and responsibilities across the organization. This process involves multiple C-level roles. The CISO must coordinate across those roles to ensure that the inherent and residual cyber risk is understood and that the C-suite shares appropriate actions in cyber program management.

Who does a CISO report to?

There are diverse reporting structures for the CISO role that reflect the organizational needs and emphasize the significance of cybersecurity leadership, which is directly

accountable to the board or business owner. Depending on the organization type, the CISO may report to any of the following:

- Chief Executive Officer (CEO)
- Chief Information Officer (CIO)
- Chief Operating Officer (COO)
- Chief Compliance Officer (CCO)
- Chief Administrative Officer (CAO)
- Chief Financial Officer (CFO) or
- Chief Security Officer.



Ultimately, the CISO is accountable to the Board or the business owner.

What kind of companies need a CISO?

Every company that uses technology to conduct business, regardless of size, can benefit from the expertise of a CISO, with considerations for full-time or fractional roles depending on your company's scale and regulatory environment. Large companies typically require a full-time CISO and small and mid-size companies can be served by a part-time or fractional CISO.

Further, the emergence of the term “vCISO” or Virtual CISO can complicate the choices and surrounding discussion. For the purposes of this document, vCISO overlaps with fractional and most often means “highly fractional,” often 1-4 hours per week in an advisory role at generally smaller companies or those with less-experienced security leadership needing a world-class mentor.

Certain regulated industries (e.g., financial services) *require* a CISO for regulated companies, with a virtual CISO (vCISO)* being an acceptable option (see New York State Cybersecurity Resource Center). If the confidentiality, integrity, and availability of data and the supporting systems are concerns, an organization will benefit from and often require a CISO.

** New York State Cybersecurity Requirements for Financial Services Companies can be found here. Section 500.4 Cybersecurity Governances states: “Each covered entity shall designate a CISO. The CISO may be employed by the covered entity, one of its affiliates, or a third-party service provider.”*

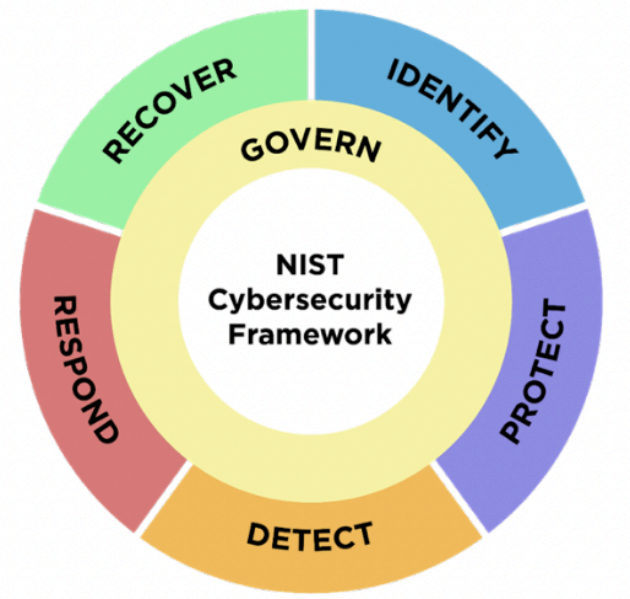
What are the key responsibilities of a CISO?

The key responsibilities of a CISO are guided by a variety of frameworks, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). These frameworks broadly cover the cybersecurity spectrum from strategy setting and

risk management to incident response and recovery. A framework ensures a robust, forward-thinking cybersecurity posture. Per NIST CSF guidelines*, the cybersecurity function must provision and manage key functions of a modern cybersecurity program: Govern, Identify, Protect, Detect, Respond, and Recover.

Specific responsibilities include:

- Setting strategy, policy, and related execution plans
- Security Risk management
- Security architecture, technology, and infrastructure
- Incident response and disclosure
- Security Awareness and Training
- Third-party (vendor) risk management assessments
- Reporting to various key points of partnership and disclosure:
    - Regulatory
    - Compliance
    - Leadership
    - Board
    - Clients
    - Employees



*Source: NIST Cybersecurity Framework 2.0

What are the key attributes of a successful CISO?

It is paramount that a CEO can identify the essential qualities of an effective CISO, including strategic insight, technical expertise, and the ability to communicate complex security issues across all organizational levels. Here is a summary of a CISO's attributes:

- Strategic thinking
- Business acumen
- Technical proficiency
- Risk management
- Clear Communication to all levels of the organization
- Collaborative management style
- Situational Awareness, and
- Adaptability.

What are some alternative titles for the Chief Information Security Officer (CISO) role?

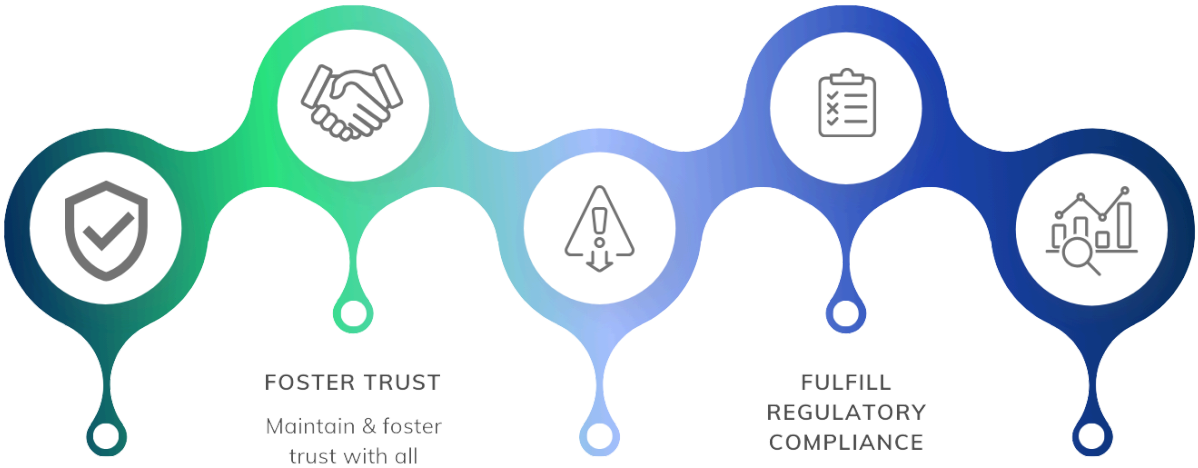
There are a range of titles that reflect the varied nature of the CISO role and highlight the adaptability and broad scope of responsibilities critical to modern cybersecurity leadership. They include:

- Chief Trust Officer
- Chief Security Officer
- Information Security Officer
- VP of Information Security
- Risk Management Officer
- Technology Risk Management Officer
- Director of Security
- Information Assurance Officer

Part 2: How Does a CISO Add Value?

The modern business landscape is fraught with cybersecurity threats, making the Chief Information Security Officer (CISO) role more crucial than ever. In this second part of our guide, we delve into how a CISO can fundamentally shift your organization's approach to security, turning potential vulnerabilities into fortified strengths.

A CISO brings immense value by safeguarding sensitive information and fostering trust among stakeholders; in an era where cyber incidents are not a matter of “If” but “when,” a CISO’s role in averting, containing, or minimizing the costs of cyber exploits cannot be underestimated. Beyond risk management, the CISO plays a pivotal role in easing regulatory scrutiny, optimizing security investments, and enhancing the overall cyber posture of your company.



A CISO adds value by providing the technology leadership needed to:

- **Protect Digital Assets**: Protect the sensitive information of the business.

- **Foster Trust**: Maintain and foster trust with all stakeholders, including customers, business partners, internal management, employees, and company leadership.

- **Minimize Risk**: In 2022, 83% of businesses had experienced a cyber incident (The Devastating Impact of a Cyber Breach, HBR, May 2023). A cyber threat represents at least a significant unplanned business cost or, at most, an existential risk to the business. A CISO averts, contains, or minimizes the cost of exploitation.

- **Fulfill Regulatory Compliance**: A CISO can significantly ease regulatory scrutiny and the associated challenges by maintaining and providing a clear view of the organization's cybersecurity posture, which instills confidence in regulators and investors alike.

- **Measure/Manage Cybersecurity**: Positioning security controls in key functional areas, such as the Application CI/CD process, can save significant time for those functions, averting significant and costly retrofit that may be required otherwise.

What are the most pressing challenges that hiring a CISO solves?

Hiring a CISO addresses several key challenges: unifying cybersecurity efforts, consolidating security resources, and providing a clear overview of security risks. This

central leadership fosters cohesion and clarity, establishing a comprehensive and strategic approach to cyber threat management.

A CISO:

- Provides central leadership and cohesion across all cybersecurity functions
- Consolidates security tools, resources, and budget
- Provides a clear view of the security risk(s) an organization is addressing/accepting
- Provides a risk-based lack of visibility into the overall cybersecurity program, and
- Presents a credible spokesperson for internal and external stakeholders.

What are the top 3 priorities of a CISO?

A CISO focuses on establishing a clear cybersecurity strategy, managing ongoing risks, and leading incident response efforts. These priorities ensure that cybersecurity measures are preventive and responsive, enabling your business to recover swiftly from security incidents. The Top 3 priorities are to

1. Maintain a clear strategy for the cybersecurity program with accompanying governance.
2. Provide ongoing risk management, including operational threat management
3. Establish incident response workflow, crisis recovery leadership, and scenario planning.

Part 3: How Does a CEO Select a CISO?

The digital frontier is constantly evolving, and with it, the Chief Information Security Officer (CISO) role becomes increasingly critical. As CEOs, selecting a CISO can be

pivotal for your organization's cybersecurity posture. In this third part of our guide, we explore the nuanced process of selecting the right CISO for your business.

Recognizing the need for a CISO is the first step in this journey. Whether due to the departure of a current CISO, a significant change in regulatory requirements, or the realization that your cybersecurity leadership is lacking, identifying the root cause is crucial. This awareness will shape your search and the specifications of the role.

Here are four steps you can use as a guide for selecting a CISO:

1. **Define** the role requirements, reporting lines, success criteria, budget, and resources.
2. **Solicit** executive and key management team members' opinions on their needs and requirements for the role.
3. **Identify** sources of CISO talent, including both full- and part-time options.
4. **Evaluate** a prospective CISO's leadership skills and cultural fit for the organization.

What type of organizational situations drive the need for a CISO?

There are several organizational situations that drive the need for a CISO:

- Lack of an executive to manage cybersecurity: An organization may lack a dedicated leader with the necessary authority and expertise to oversee and direct cybersecurity initiatives.
- Departure of current CISO: If an organization's current CISO leaves, it creates an immediate gap in cybersecurity leadership that needs to be filled to maintain security posture.
- Current cybersecurity leader is ineffective: If the existing cybersecurity leadership is not meeting the organization's needs, a change may be necessary to better protect digital assets and comply with regulations.

- Organizations operating market or regulatory needs have changed significantly: If there have been significant changes in the market or regulatory requirements, an organization may need to hire a CISO with specific expertise to address these new challenges effectively.

These situations underscore the importance of having a competent and dedicated CISO to navigate the complexities of modern cybersecurity challenges and regulatory environments.

What experience, spend, and availability are required?

Before considering the experience, spend, and availability required to hire an interim, fractional, virtual, or full-time CISO, there are a few areas that the leadership team needs to establish for common ground:

- What is your organization expecting from a CISO?
- Has the executive team agreed on the job description and the roles & responsibilities for the position?
- What are the success metrics for a new CISO six months into the role?
- What are the success metrics eighteen months into the role?

The ideal CISO should bring a rich tapestry of experience, ideally with previous CISO roles or significant leadership in technical or risk management. By seeking a technology leader with the demonstrated ability to scale a security program, your organization will be able to adapt to ever-changing technology and regulatory requirements. The ideal fit would be to match that CISO´s experience with your organization's sector and size.

However, understanding the financial commitment is equally important – from competitive compensation to the overall cybersecurity budget. Another consideration could be to evaluate what, if any, non-monetary compensation your organization may be

prepared to offer. Lastly, consider the availability of candidates who have the experience and can address current cybersecurity priorities effectively.

With an understanding of what is driving the need for a new CISO, a CEO must consider the following:

- Experience: What CISO **experience** does the organization require? ,
- Spend: What can the organization afford to **spend** for that experience? & What can the organization afford to spend on the technology function as a whole? and
- Availability: What type of candidate **availability** is required?

Experience

The ideal candidate would have prior CISO experience or C-level experience in a Technical or Risk management role. Such requirements may include, although are not limited to:

- Deputy CISO or senior manager cybersecurity experience may be suitable.
- Minimum of 5 years in a senior management role.

The ability to be conversant about cybersecurity priorities and track current trends and issues is also a critical priority as the cyber landscape changes each year.

Spend

What an organization can afford or is willing to pay for the CISO role can significantly impact the CISO they can attract. It can also signal how the organization perceives the CISO role. While it is instinctive for most organizations to default to full-time employment, CEOs should be aware of alternative approaches to solving for technology leadership that offer on-demand, as-a-service models providing full-time, part-time, short-term, and long-term engagement that maximize experience within the three dimensions discussed above. The right amount of technology leadership spend is that

amount of money that will attract the most experienced leader the organization can afford - including through fractional and interim assignments.

The overall budget for cybersecurity programs can range from 5% to 15% of the total IT budget in larger organizations. Note that if an organization has not invested any budget line item in its cybersecurity initiatives, it should expect a larger budget in the first two years to align with best practices.

Availability

An organization's needs driving the hiring of a CISO may impact the number of possible candidates based on their availability in two areas:

- **Availability to start** - Most searches at the executive level can take 6-9 months. If the organization has strong secondary leadership in place or engineers an orderly transition with the existing technology leader, a 6–9-month search may not be an issue. However, if a prolonged CISO vacancy disrupts the organization, puts the continuity of technology initiatives at risk, or prevents the organization from pursuing impactful new technology initiatives, a 6- to 9-month search may pose a big problem. An interim (full-time) or fractional (part-time) CISO is the best option when near-immediate availability is needed. An added benefit of the interim and fractional CISO relationship with no long-term commitment is that there is often less resistance to getting started quickly. In contrast, the perceived need for greater due diligence for a "permanent" role will cause the organization and the candidate to move more slowly.

- **Availability to engage in a variety of ways** - In addition to the immediacy of availability, the organization may need the availability for a candidate to engage in ways beyond traditional full-time employment. Not every CISO is interested in, comfortable with, or qualified for fractional or interim roles. CISO candidates with

more experience, greater financial stability, higher risk tolerance, and an entrepreneurial spirit may be more appropriate for interim or fractional roles.

What are the hiring approach options?

The previous two sections encouraged CEOs to think holistically about the organizational need driving the selection of a new CISO and reflect on the required experience, spend, and availability before selecting a hiring approach. While executive search remains the most familiar hiring approach, knowing all options empowers CEOs to make the best choice for their organization's short- and longer-term needs. This section reviews the Executive Search and Leadership-as-a-Service approaches to finding a CISO.

Executive Search - Search to Own

Retained executive search firms take a consultative approach to understand an organization considering a search to fill an executive role. The consulting process ensures that each client receives their full attention to craft search priorities and a search strategy that considers their unique needs for the role and the leader. A reputable firm will often understand the organization's culture, explore the reasons for the vacancy or new role, and become aware of any HR guidelines for the candidate. They may also develop insight into the personalities, work styles, and preferences of the CEO and the intended role's peers and spend time crafting a detailed job description and candidate profile specific to the client's organization. Successive interviews and feedback lead to selecting a preferred candidate who, hopefully, accepts the offer and transitions into the new role as a full-time employee.

Larger search firms have specialized practices for specific roles, and some search firms specialize entirely in roles within a particular domain, such as Finance, Technology,

Human Resources, etc. Fees for retained executive search services typically amount to one-third (33%) of the candidate's first-year cash compensation, including the base salary, signing bonus, and any other projected bonuses. The fee is paid in equal installments upon the start of the search, 60 days into the search, and following the acceptance of an offer by a candidate. For a CISO, this acquisition cost amounts to approximately 7% of cash compensation over the average tenure of 4.6 years (as of 2019). It does not include the cost of equity compensation, benefits, severance, and ongoing employment costs. The time to conduct a search varies but averages between 3 to 9 months from the start of the search to the candidate's start date, during which the client is usually without leadership in the role.

Leadership-as-a-Service - Access over Ownership

Leadership-as-a-Service (LaaS) is a managed service that allows an organization to engage vetted, world-class executive leaders in as little as a few days to 2 weeks. Technology Leadership-as-a-Service^{R} (TLaaS^{TM}) is the LaaS concept applied exclusively to the CIO, CISO, and CISO roles. In most cases, executives of firms offering Leadership-as-a-Service have decades of experience *in* the role they are offering. Combined with the tens or hundreds of executives serving their clients in those roles, they are also experts *on* the role. Role-based expertise and a ready supply of available executives can dramatically reduce the time needed to fill a vacancy or apply senior talent to an important initiative. Technology leaders in a TLaaS model enjoy association with tens or hundreds of other technology leaders incentivized to help one another serve clients in ways that no single technology leader can achieve alone - employed or not.

TLaaS may be appropriate when an objective review of the organizational needs, required experience, spend, and availability allows for a CISO in an interim or fractional role. TLaaS may also offer a CISO in a situational leadership capacity to facilitate an important initiative such as an assessment, transformation, or consolidation for a specific outcome.

- Fractional CISOs engage for 1-2, 2-3, or 3-4 days/week, and the relationship is generally open-ended - continuing as long as the arrangement works for both the client and the leader.

- Interim CISO roles are full-time and generally assumed to end when a full-time, employed CISO is found - usually through executive search. Hybrid models allow a fractional or interim leader to be an employee of the client without requiring a long-term commitment while remaining connected to the larger community of technology leaders. Finally, most Leadership-as-a-Service firms offer a path to becoming a full-time employee of the client for a placement fee.

In contrast to up-front fees for executive search, Leadership-as-a-Service embeds fees for the leader in the monthly cost. Fees only last as long as the leader provides the needed value and can increase or decrease in response to the natural rhythm of innovation and stability over time. Models vary, but a general rule of thumb is that Leadership-as-a-Service costs, on average, about 20% more than the base salary of an equivalent leader in a full-time role. However, the cost of a CISO for 2-3 days per week with more experience across all three dimensions without hiring risk may be similar to, or less than, the combined acquisition, ongoing, and severance cost of a full-time, employed, possibly less-experienced, CISO with the associated hiring risk.

Executive search offers a custom approach to finding a perceived perfect fit for an expected long-term role. In contrast, Leadership-as-a-Service provides a ready pool of experienced leaders for immediate engagement under flexible terms.

How does the CEO make a final selection for a CISO?

After considering the organizational need driving the selection of a new CISO, reflecting on the required experience, spend, and availability, and reviewing the two approaches

to hiring a CISO, the CEO will need to choose a hiring approach and make a final selection of a CISO. The good news is that either approach can produce equally qualified and effective CISOs. The right choice for a given organization, in a particular situation, at a given time will influence the hiring approach and final CISO selection. The Executive Search and Leadership-as-a-Service options are covered below.

Choosing Executive Search

The retained executive search model may be the obvious choice if the organization:

- feels most comfortable with a traditional search,
- the assessment of the needs, required experience, spend, and availability suggests a full-time, employed CISO is best and
- there is confidence in the organization's ability to match a candidate's capabilities with the organization's needs.

Select a Search Firm

There are over 5,000 search firms in the United States and 20,000 or more worldwide, so there is no shortage of choices. The more specialized the firm, or a practice within a firm, is toward the CISO role and possibly even the CISO role within a given industry, the more likely the firm will be familiar with qualified CISOs when the firm reaches out to discuss the role. Demonstrated experience completing CISO searches with references to satisfied clients is a must. The search process is long, involving many hours of discussing the role, the profile, the candidates, and the offer strategy. Finding senior leaders and associates of the firm that match the organization's values and are enjoyable to work with can make the entire process more pleasant.

Frame up the Role

The search process emphasizes crafting a specific profile that will be most successful in the role at a given organization. Great care is taken to get input from multiple sources

to arrive at a composite profile representing the perfect candidate. Finding the ideal candidate is a great goal, but the CISO role is relatively static across organizations and industries at any given time. Don't get creative in defining the role. A great CISO knows how to be a CISO and is a living profile. Value candidate experience and tenure most.

Evaluate Candidates

The highest predictor of success in a CISO role is past success in a CISO role and is likely not unique to the organization. When evaluating CISO candidates, consider the following observations:

- Success in the CISO role is best reflected by the number and duration of CISO roles served. There is no substitute for experience "in the seat," and change teaches lessons. More CISO role experience is better than less CISO role experience. Place the most value on candidate experience.
- Assume leadership in prior organizations acted rationally, keeping successful CISOs longer and exiting unsuccessful CISOs sooner. Also, assume CISOs acted rationally, staying longer in circumstances where they could be successful and leaving those where they could not. There are exceptions, of course, but assuming rational behavior is a good start.
- The success of a CISO of any given organization is highly dependent on factors outside of their control. What worked in one organization at a specific time, with certain people under particular circumstances, may not work in another where all those factors are different. Adaptability is necessary to succeed anywhere, but some organizations contribute more to the failure of the CISO role than the CISO themselves. Not all such claims by candidates are excuses.

Make the Selection

The average tenure of a CISO in 2023 was only 18 months - much shorter than their C-Suite counterparts (source: Enterprisers Project). In addition, Gartner predicts that half of all CISOs will be changing jobs by 2025. Thus, even though CISOs remain in high demand, organizations cannot eliminate all hiring risks. Select the most experienced candidate available at the time and emphasize being an organization that can contribute to CISO success and commit to early detection of, and fast response to, a poor fit (e.g., fail fast).

Choosing Technology Leadership-as-a-Service

If the analysis above fails to suggest a definite choice between Executive Search or Leadership-as-a-Service, or the potential to immediately engage a world-class, full- or part-time CISO with little hiring risk is attractive, Leadership-as-a-Service is a compelling choice.

Selecting a Technology Leadership-as-a-Service Provider

There are far fewer individuals and Leadership-as-a-Service firms offering fractional and interim CISO services than there are search firms, so finding one may prove more challenging than engaging one.

- A CEO's personal network is a good source of referrals, including other CEOs, Board members, Private Equity and Venture Capital investors, past colleagues, trusted advisors such as attorneys, CPAs, bankers, consultants, executive peer group chairs and members, and other leadership-as-a-service providers offering finance, marketing, legal, human resources, and operations leaders. Another option is to check the major search engines for relevant terms such as "interim CISO," "fractional CISO," or "virtual CISO" (a highly fractional advisory CISO role).

- Among the referrals or search results, value the number and breadth of individuals available to provide CISO services. A single individual can be an excellent choice if they are available and interested in the work. A larger firm with tens or hundreds of resources will provide more choice, is more likely to have experience specific to a given industry or situation, can more readily offer additional or different resources as needed, and increases the effectiveness of any given CISO through a vibrant community of fellow technology leaders. A firm with many resources indicates that its business model is attractive to the CISO and that there are enough clients to keep them as busy as they want.

- With a short list of individuals or providers, visit their website, check LinkedIn, and contact their leaders via chat or email to start the conversation. Get a feel for their experience, connections, and the quality of their online presence. A successful provider will offer education online, respond quickly, and be ready and willing to help solve the need for a CISO or advise on alternative solutions.

- An initial discussion with a leader with extensive experience helping organizations evaluate and select fractional and interim CISOs will uncover specific requirements and prompt deeper dialog about the CISOs that will produce the best fit among available resources.

- Based on the organization's preferences and the number of resources fitting the request, the provider presents one to three technology leaders with associated biographies and experience. Some situations may prompt a proposal covering the understanding of the situation, the approach to solving the need, and a discussion of the proposed people.

- If a proposed CISO is acceptable, an agreement between the organizations is signed. The new CISO may start as soon as the CISO and client can arrange a mutually agreeable date.

Getting Started with Technology Leadership-as-a-Service

Most fractional and interim CISO providers will be able to get started very quickly, often providing viable candidates within hours to days and beginning within one to two weeks if speed is essential.

Leadership-as-a-Service in Action

Once the fractional or interim CISO starts, they start doing what CISOs do - assuming responsibility and accountability to support the organization. Generally, they operate like any CISO - attending leadership and Board meetings, providing status updates, managing the technology organization, interacting with customers and vendors, and carrying out the responsibilities and priorities of the CISO role. Interim roles are full-time and expected to be available just as any executive would be. Fractional roles are part-time and expected to be available on a regular, agreed-upon schedule and as-needed on a best-efforts basis. Fees are usually invoiced monthly or twice monthly. Larger firms have sufficient resources for ongoing contact with the firm's leaders as necessary and administrative support for resolving issues and smooth operation. Fractional and interim roles can be short-term or extended for years when there is a good fit, and the organization believes the value proposition meets its needs.

As mentioned above, even if the organization has chosen Technology Leadership-as-a-Service to solve their technology leadership needs for a particular time or situation, Executive Search is often used to find a full-time employee. Most providers have good relationships with search firms and can make a referral when needed.

Combining Technology Leadership-as-a-Service and Executive Search

Executive Search and Leadership-as-a-Service are not entirely mutually exclusive. Executive search is almost always part of the interim CISO process and can be a part of

the fractional CISO relationship when it's time to transition to a full-time employee. The fractional or interim CISO can be one of the most objective and qualified participants in the search:

- Having spent ample time with the CEO, Board, and peer executives, they understand what it will take for the new CISO to be successful and what the organization must do to contribute to that success.

- Based on a deep personal understanding and working knowledge of the organization's needs, they can help evaluate candidates to determine the best fit. They can also be an informed and technically adept voice to the potential candidate to help them understand the opportunity, give insight into the organization and its people, and describe any specific capabilities or approaches needed to succeed.

- If all parties agree, the fractional or interim CISO can continue to provide services through the transition to give the new CISO extra time to focus on the most critical issues or even act as a force multiplier to augment the new CISO's capabilities to tackle some important initiatives.

Even if the organization has started an executive search and has not engaged a fractional or interim CISO from a Leadership-as-a-Service provider, it's not too late! Doing so will take some pressure off the organization to make a quick decision, provide reassuring coverage for the role while the search is ongoing, and, as explained above, can contribute positively to the search and transition after selection.

Contributors: Burke Autrey (CEO), Walt Czerminsiki (Partner), Tim Mather (Partner), Bill Alfveby (Partner).