How To CISO

The Idealized CISO

How to CISO Volume Zero

V1.1: 2024

The Idealized CISO 2
Executive Summary 2
The Security Executive 3
- Security Expert 3
- Enterprise/IT Security 3
- Security Operations 3
- Incident Response 3
- Platform Safety/Security 3
- Threat Intelligence 4
- Compliance 4
- Risk Management 4
- Corporate Governance 4
- Board Reporting 5

The CxO 6
- Organizational Leader 6
- Financial Planner 6
- Effective Partnerships 6
- Cyber Risk Advisor 6

The Go-To-Market CISO 7
- Product Strategist 7
- Thought Leader 7
- Field Marketer/Evangelist 7
- Sales Enabler 7
- Sales Closer 8

The CIO 9
The Chief Physical Security Officer 9

The Idealized CISO

If a company could design a perfect CISO, they would be able to seamlessly move between multiple disciplines, filling a number of critical roles. While no individual is likely to actually fill all of these roles, it's valuable to understand all of the possibilities, to assess the development needs of the incumbent against all of the *possible* aspects of their job. "The CISO" below may refer to the CISO as an individual, or to a person or team in the CISO's organization who fulfills that role.

Executive Summary

Many companies are not in dire need of a CISO *right now*, but need to define a role for their future CISO, often including a plan to develop the incumbent security executive into a credible CISO. This guide provides a profile of the idealized CISO. Why ideal*ized*, and not *ideal*? Because a CISO is often viewed as a multidisciplinary master of all trades: not merely a unicorn, but an entire herd of unicorns. Understand that this job description is *too* comprehensive, and serves as a conversation starter around the role of the CISO and the role of their team.

A search for an ideal Chief Information Security Officer (CISO) will present significant challenges, primarily due to the highly specialized skill set required for the role. The pool of candidates who fully match the idealized CISO profile is vanishingly small. Moreover, the likelihood that these candidates are both available and willing to take on this role at a given company is, functionally, non-existent.

Given this scenario, companies should remain open to potential opportunities to recruit an external candidate, as is prudent for any executive-level position. However, many companies have an incumbent security leader with many of the necessary qualifications and company-specific knowledge; that incumbent *may* be a good candidate to develop into the ideal CISO for the future.

The Security Executive

In most organizations, the CISO's primary function is as the senior security executive. In this role, they juggle a number of responsibilities, serving as the first, and also last, person responsible for security. They will define and drive forward the company's security posture, culture, and strategy.

Security Expert

The CISO is often expected to be the expert on all things security, with a wide range of domain knowledge, and the ability to quickly assess security risks on complex systems with little or no preparation. They need to have a deep understanding of a wide variety of security disciplines, be able to propose solutions to address the security challenges presented by new business ideas, and understand the feasibility of implementing those solutions within the current organization. The CISO also needs to understand where the limits of their expertise ends, and incorporate the expertise of others into their decision-making.

Enterprise/IT Security

The CISO often plays a crucial role in defining the security strategy for the corporation's information security (separate from the *business*, which involves the product/platform). This includes the development and enforcement of security policies and procedures, leading security awareness training programs, and spearheading risk management strategies. The CISO acquires, deploys, and operates both first and third party security technologies, integrating those technologies together and with first-party systems, to ensure a cohesive and robust security posture for the corporate ecosystem.

Security Operations

The CISO is responsible for overseeing the security operations of the organization, either directly through their organization, or by governing other operations teams. The CISO ensures that security technologies are correctly functioning, that security alerts are handled appropriately, and that users are supported in their day-to-day security interactions.

Incident Response

During a security incident or breach, the CISO often takes the role of Incident Commander/Incident Executive, guiding the company through remediation, crisis communications, and recovery efforts. To prepare for the (hopefully rare) occurrences when this happens, the CISO coordinates incident response planning, tabletop simulations, and relationships with external entities such as law enforcement and crisis management teams.

Platform Safety/Security

Any infrastructure/SaaS business operates on a shared platform, and the CISO often represents the primary voice to ensure that platform meets the safety and security needs of the customer. This responsibility is similar to the resilience, performance, and scalability responsibilities that often sit with a CTO, head of Engineering, or CPO: needs that customers implicitly have, but

rarely articulate. The CISO defines a coherent security strategy for the platform, and then works primarily through influence to gain strategic buy-in. Once a strategy is set, the CISO shepherds it forward, ensuring the platform architecture is always improving.

Threat Intelligence

The CISO must remain up-to-date not only on security technologies and practices within the security community, but also on the advances being made within the adversary community. The CISO must be able to coherently provide threat modeling in support of designing safe and resilient systems, and understand when the changing adversary ecosystem needs to prompt defensive design changes within the company's practices.

Compliance

The CISO ensures that the organization not only adheres to applicable legal and regulatory requirements but also to industry standards and best practices concerning information security and privacy. This involves a comprehensive understanding of the regulatory landscape, which can include international, national, and industry-specific mandates. The CISO's responsibilities in compliance extend to orchestrating audits, managing certifications, and maintaining evidence in support of compliance efforts. Additionally, the CISO is instrumental in integrating compliance requirements into security policies, procedures, and technologies, aligning them with the organization's risk management strategies.

Risk Management

Risk Management is a critical aspect of the CISO's role, involving the identification, assessment, and prioritization of risks to the organization. A key part of this process is educating and collaborating with other executives to ensure they have a coherent understanding of security risks and their potential impact on the business. By effectively communicating the nature of these risks, their plausibility, and potential consequences, the CISO enables other leaders to make more informed decisions in their strategic planning. This often involves translating complex security concepts into business terms, demonstrating how security risks can affect business objectives, and proposing strategic options for risk mitigation. The goal is to foster a culture of risk awareness and to ensure that executive decision-making is aligned with the organization's risk appetite and security posture, thereby enabling the organization to make wiser choices regarding risk tolerance and mitigation strategies.

Corporate Governance

Tying together all of the elements above, the CISO is responsible for orchestrating the company's security efforts and leading the company's security culture. Tracking key metrics, understanding and communicating deviations from the company's security philosophy, and driving security programs forward across the business, the CISO represents the central coordination and communication point for all executives to feel confident that they understand the company's security posture, and that the posture matches their understanding.

Board Reporting

The CISO bears the responsibility of a regular report to the Board. Through this report, the CISO ensures that the Board is able to execute on good governance: verifying that the company is taking appropriate steps to manage risk commensurate with the risk tolerance of the business. The CISO must be able to operate at a high level in the boardroom, educating the Board on the risk posture of the company, the security initiatives underway, and progress against key metrics. The CISO must also be a security expert for the Board, putting current news events about security into a corporate context.

The CxO

In many organizations, the CISO is not truly a C-level executive. Often reporting one or two steps away from the CEO, the CISO needs to *react* to decisions after executives have made them, trying to inject security and risk management perspectives upstream into an organization that is already moving. To truly be a C-level executive, a CISO needs to not only be in the "room where it happens" as part of the CEO's staff, they need to be able to operate as a corporate executive in that room *first*, and as the voice of security *second*. This is a hard and difficult transition for many CISOs to make, holding what seems like two contradictory requirements in hand at the same time. Every CxO needs to do the same; balancing the domain expertise and organizational responsibilities into the room, while helping the business make wise choices for its future success.

Organizational Leader

The CISO must be an effective organizational leader. In addition to the common requirement on all executives to lead and guide their organizations and people to success, the CISO bears an additional responsibility, as they must be able to develop security expertise within their team, and ensure that the security philosophy of the company is shared by all of the organization's security experts. While this responsibility is often similar to other organizations, the willfulness of many security professionals adds a layer of complexity onto achieving this objective.

Financial Planner

Like any CxO, the CISO needs to understand the financial dynamics of their organization, and consider the long-term effects of any budget outlay. No longer is it sufficient (or even prudent) to tactically engage in budget conversations with a return on security investment (ROSI) calculation to drive a single project forward. Rather, the CISO must plan years out for their budget and priority plans, while applying financial agility to tackle problems in real-time as priorities shift.

Effective Partnerships

A great CxO understands a bit of every adjacent domain. A CISO who excels should understand and value the roles and responsibilities of their peers: revenue, marketing, legal, finance, people, engineering, and products. The CISO should be able to proactively address the security needs of their peers, while helping them advance the business.

Cyber Risk Advisor

The CISO enables other business leaders to make more effective decisions by providing timely and relevant risk advice, helping to guide the company quickly away from untenable strategies, and on to more fruitful paths. A key component of being the Cyber Risk Advisor isn't just managing a massive spreadsheet of risks – it's understanding which risks can be mitigated with cost-effective work, in a way that will also advance the business, and putting that risk into the language that the CISO's business partners will understand.

The Go-To-Market CISO

Any company that is selling a form of trust to other enterprises often needs their CISO to participate in their overall marketing strategy, even if they aren't specifically a security vendor. The CISO needs to be able to articulate appropriate and trustworthy security messages tailored for different environments and listeners. Sometimes decoupled from the CISO role, this position becomes an Advisory CISO, CISO Evangelist, or Field CISO; at large scale, the company may employ one or more individuals just in this role.

Product Strategist

In a cybersecurity company, a CISO often serves as a shadow advisor to the CTO or head of Product Marketing. By understanding the buyer mindset, and being able to provide rapid and unvarnished feedback on product requirements and features, the CISO can reduce the time to achieve a strong product-market fit in a company. While the power of external customers serving in the role of advisors should not be underestimated, the view of an insider can be indispensable. The CISO should be able to separate their risk hat ("don't do anything dangerous") from their role as an executive ("bring in valuable revenue") to succeed well in this role.

Thought Leader

In their role as industry thought leader, a CISO has novel and interesting viewpoints that other security professionals find valuable. Many of these viewpoints should not be directly adjacent to the business's product area; the purpose of the CISO as thought leader is to establish the CISO's brand as one which is interesting and trustworthy (by adjacency, the employer's brand is also heightened). Some of the viewpoints should be near the business: discussions of security lessons learned in operating this business, conversations about distributed system safety, guidance on building a security team at scale. In their role as thought leader, a CISO often exists in tension with tactical field-marketing teams, who focus more on creating demand than on building corporate brand; but the thought leader CISO is a valuable asset to corporate PR.

Field Marketer/Evangelist

The CISO represents a valuable asset to all aspects of messaging and content generation: an internal focus group (of one) who can pressure test what content might resonate with the CISO community, identifying objections before they become blockers to deals. While security companies might need the CISO as a deep part of their messaging strategy, non-security infrastructure and services companies still gain value from crafting messaging that turns the security stakeholders in target customers from objectors to advocates. The CISO should be able to represent the company at marketing events, from giving talks at conferences to hosting dinners or parties at conferences.

Sales Enabler

The CISO should serve as a mentor to all stages of the Sales organization, helping them to understand more effective go-to-market activities. An Inside Sales team benefits from practicing

their pitches on the CISO, while an Account Executive can use the insight of the CISO into the nuances of a specific company or prospect CISO to tailor their approach.

Sales Closer

A key role of the CISO in almost every services business is to *help close deals*. Sometimes this is by providing introductions to a sales team; when the CISO engages with their community, they keep their ear out for potential prospects, and provide warm introductions to the relevant sales team. The CISO also joins an account team as needed to provide credibility and a title match when selling to a senior executive; the same sales message, echoed by a C-level executive, carries more weight with another C-level executive, and often creates an opportunity for the prospect to open up more about their needs than they'd be comfortable doing with just a sales team in the room.

The CIO

A few years ago, almost no description of the Ideal CISO would include “CIO” in the summary of roles, but the world is changing. Relatively young technology businesses often have no large IT footprint. Employees use laptops, with a SaaS backend for most traditional corporate needs; Engineering supports its own development environment. The primary needs for corporate technologies are usually driven by a bevy of security acronyms: EDR, SSO, IAM, *SPM, VRM, TPRM. As the CISO increasingly supports more of the corporate information technology, the need for a separate CIO diminishes. To fill the role of the CIO, however, a CISO isn’t merely the “securing all the data.” They need to become the technology business partner for the business; helping different parts of the company select and (safely) implement technologies in support of their functions, while monitoring the overall company technology strategy to ensure it is both aligned and cost-effective to the business.

The Chief Physical Security Officer

The CISO often bears additional responsibilities around forms of physical security, especially in companies without a significant physical footprint: securing the workplace, providing executive security, and coordinating security for travel into certain nations. In the workplace, the CISO needs to not only consider the appropriate technologies for building access and surveillance, but also tie those into the overall information access philosophy. Many executives, especially at publicly traded companies, require either digital or physical safety services, and the CISO may be the appropriate coordination point for these services. The CISO must also coordinate the security strategy around corporate travel to nations which routinely engage in business espionage (e.g., China, Russia), ensure that both traveler awareness and device protection are handled appropriately.