THE EVOLVING ROLE OF THE CISO

MORE THAN JUST SECURITY

OCTOBER 2023

U.S. Cybersecurity Group

ASPEN DIGITAL

aspen institute

INTRODUCTION

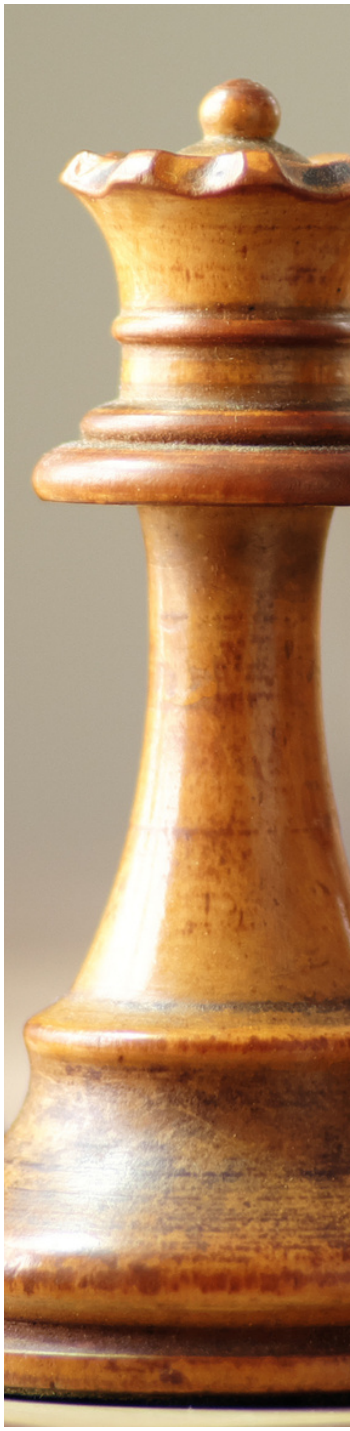
VISIT OUR WEBSITE
aspendigital.org

For years, many have seen the Chief Information Security Officer (CISO)[1] as only a technical advisor to the C-suite– the CISO counts vulnerabilities and assesses patching status, provides a progress report on the same to other executives, and then leaves the business risk questions to strategic advisors and decision-makers. If this ever was an accurate description of what a CISO does – or should do – it is no longer sufficient. Systemic shifts within and outside of the business environment have changed the role and responsibilities of the typical corporate CISO for good.

Nonetheless, a central and constant objective of all CISOs is still to protect the security, confidentiality, integrity, and availability of an organization's information and infrastructure, and, by extension, its entire operations. Because of growing corporate reliance on information technology systems for business operations; the rising threat of cyberattacks from criminal and nation-state actors; and expanding institutional and positional legal liability, the CISO now faces a more complex set of challenges internally and externally. Unfortunately, they often do so with the same limited set of authorities and protections they had before most organizations viewed cybersecurity as an executive enterprise risk level concern.

1. The report uses the term CISO as a shorthand for CISOs as well as other IT security function leadership positions.

Too often there is a fundamental divergence between the responsibilities CISOs bear and the authority they are given to fulfill those obligations. This divide is exacerbated by a lack of understanding among board members and senior executives regarding what CISOs do, the scope of their authority, and how their role supports organization-wide missions. Together, these structural barriers make it more difficult for CISOs to achieve their core objective and for organizations to protect their data, operations, and achieve their business mission.

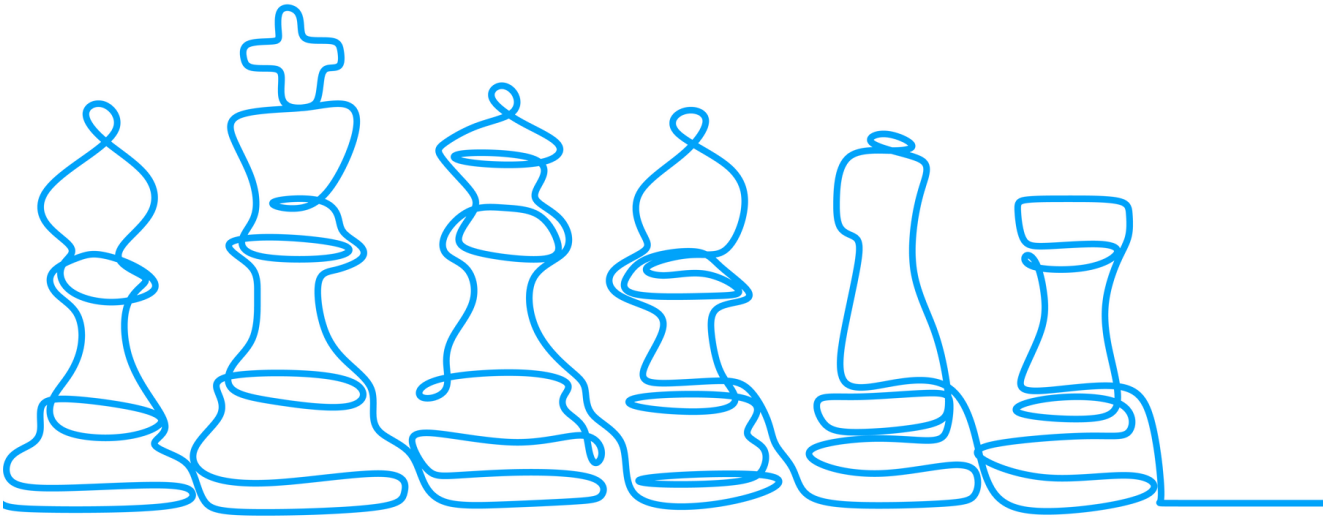


This report seeks to provide context on the current expectations and responsibilities placed on corporate CISOs; describe how those responsibilities reconcile with the authorities CISOs generally have and realities they face on a day-to-day basis; and provide high-level, structural recommendations on how business organizations can ensure that their CISO is equipped to protect business systems and achieve institutional objectives in this changed environment. The report is designed to be accessible to the general public, and also to be a tool for CISOs, corporate executives, and board members to assess whether their organization, and their CISO, is structured to be able to address the range of cyber-related risks entities grapple with on a daily basis.

The report recommends that organizations:

- Ensure CISOs' authority align with all aspects of an organization's business functions
- Include CISOs in senior level strategy, governance, and risk management processes
- Ensure CISOs have a role in decision-making for large-scale business, product, and procurement decisions
- Ensure CISOs have access to senior leaders and board members, regardless of the organization's specific reporting structure[2]

While the report's recommendations are designed to help organizations meet their business missions, they also help support broader national-security objectives. Private sector entities remain on the frontlines of cybercrime and conflict, and ensuring CISOs have the authorities they need will also help bolster the broader national security infrastructure.



2. While the observations and recommendations outlined in this report reflect a focus on private sector entities, many are applicable to government CISOs.

TABLE OF CONTENTS

THE STATE-OF-PLAY

CURRENT EXPECTATIONS AND TYPICAL RESPONSIBILITIES PLACED ON CISOS (AND GAPS)

"[CISOs] are given this responsibility, but not the resources, influence, or accountability to ensure that security is appropriately prioritized against cost, performance, speed to market, and new features. When cybersecurity is considered a niche issue, rather than a foundational business risk, organizations are not motivated to be part of a broader solution."

– CISA DIRECTOR JEN EASTERLY AND EXECUTIVE ASSISTANT DIRECTOR ERIC GOLDSTEIN IN FOREIGN AFFAIRS

1. RISK MANAGEMENT

CISOs often are responsible for managing a variety of digital risks, whether those are prospective harms the organization creates itself or ones an entity inherits through partnerships with third parties.[3] In addition, many CISOs are responsible for the security of non-digital company assets, including physical infrastructure, IoT devices, OT devices, and more. Beyond the traditional CISO functions – such as vulnerability management, endpoint protection, network protection, and cyber education – the modern CISO must engage with multiple risk and business strategy-related functions in an organization, including:

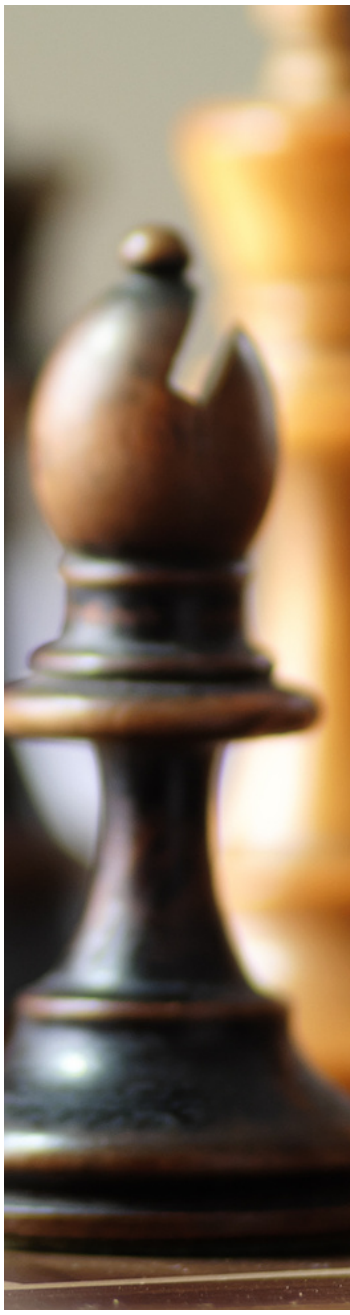
a. Procurement

Despite these risk-related responsibilities, organizations do not always integrate the CISO into procurement processes and decision-making for the assets and operations often at the center of the risk. This includes the selection of third-party vendors and outsourced operations.

3. For example, as more security tools are deployed in-line, and as cyberattacks such as ransomware and DDoS attacks grow in frequency and magnitude, cybersecurity has become an integral component of an organization's business continuity and disaster recovery functions. Cyber resiliency and cyber insurance are increasingly a part of a CISO's remit.

b. Budgeting

Even though CISOs are often responsible for a range of digital and physical risks to security, they do not always have decision-making authority over security purchases. The Chief Information Officer (CIO), or another C-suite executive to which the CISO reports, often retains this power. And even when CISOs do have some purchasing and budgeting power, it is over only a subset of the business infrastructure that presents information security risks.



c. Internal and External User Policies and Behavior

Even though CISOs are responsible for the consequences of a range of internal and external user behaviors, they often are not fully empowered to establish the secure processes by which users are required to engage with the technology that might presentt information security risks. For instance, the CISO might not be responsible for setting internal expectations regarding device usage and connectivity to applications and might not have input into the policies and processes that govern how developers create and store source code, both of which create security risks the CISO or IT security function might be responsible for.

d. Perception

Some organizations see the CISO as responsible for only enterprise-related security (e.g., workforce devices, back-office systems, etc.). In reality, the typical private sector CISO must manage external systems and security risks, including (and often especially) risks presented by third party vendors.

2. GOVERNANCE, REPORTING, AND LIABILITY

CISOs often must answer to customers, regulators, and internal stakeholders regarding their organization's information security practices and posture. This includes the responsibility to notify external parties of reportable security incidents. As a result, CISOs need to balance activities with multiple avenues for accountability, which creates challenges and risks specific to the position. Such activities, risks, and the stakeholders to whom CISOs are responsible include the following:

a. Institutional Governance and Oversight

CISOs often are not included in the highest level of governance and oversight practices of an organization (e.g., executive staff meetings, board meetings, etc.), which can lead to a knowledge gap between the CISO when she speaks externally and the board and CEO. This also exacerbates the problem of senior executives and board members not fully understanding the role and responsibilities of their CISO or IT security function.

b. Reporting Security Incidents and Critical Vulnerabilities

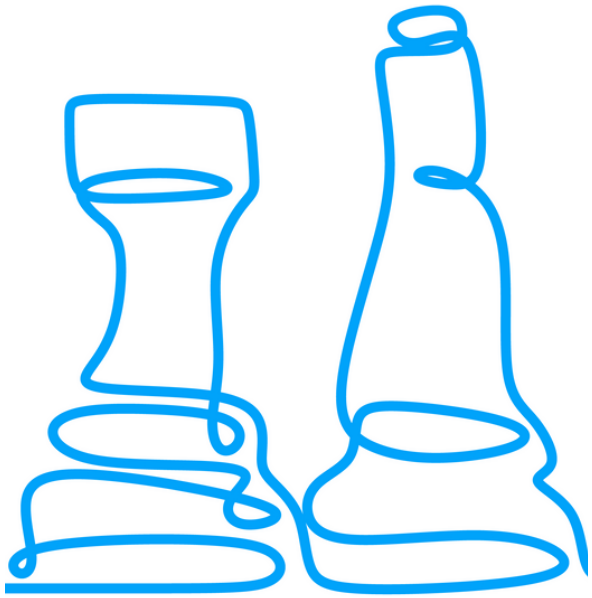
Even though CISOs, often in coordination with general counsels, typically are responsible for notifying internal and external parties about reportable security incidents and critical vulnerabilities to products, this reporting is not always visible to CEOs and board members. As a result, senior executives might not fully appreciate the scope of this duty, and therefore might not fully understand the risks an organization is grappling with. In some organizations the decision not to inform senior management may be circumvented by others in the organizations with higher authorities.

c. Personal and Positional Liability

Increasingly, CISOs are open to personal liability for actions taken or not taken in their roles, increasingly with respect to whether, how, and when an organization discloses security incidents and critical vulnerabilities to government officials and other third parties.[4]

d. Regulatory Compliance & Certifications

CISOs and their teams are often required to manage a wide variety of compliance certifications and attestations at the international, federal, state, and industry level. This requires the CISO to work across many compliance and governance functions within the company to accomplish the certification work and interface with many external parties – including customers, shareholders, insurance providers, auditors, regulators, and industry organizations.

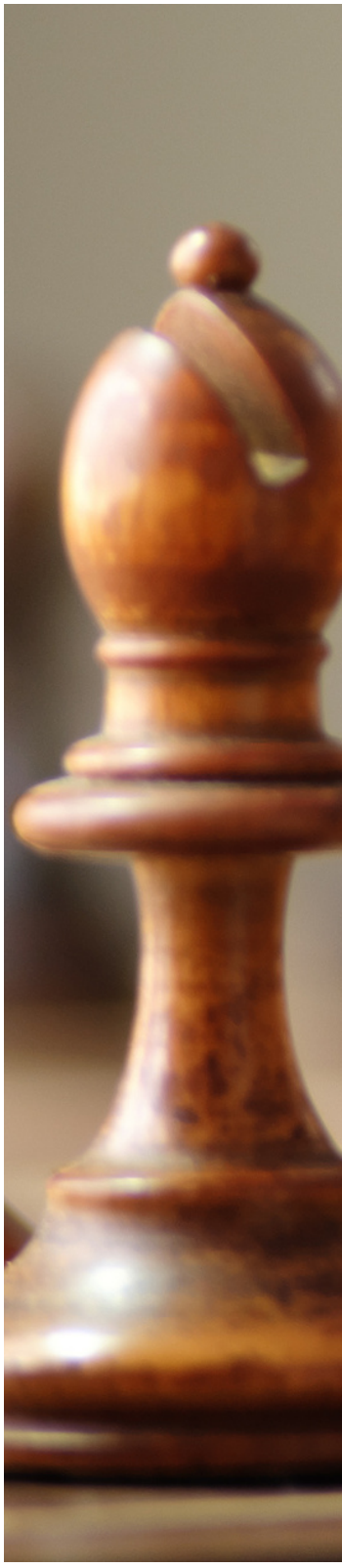


4. This includes the prospect of criminal liability as well as the possibility of civil enforcement action by entities like the Securities and Exchange Commission.

RECOMMENDATIONS

SCOPE AND SCALE OF NECESSARY RESPONSIBILITIES

In order to ensure that CISOs have the power to assess and respond to all varieties of corporate risks before they materialize, organizations must fully integrate CISOs into procurement and purchasing decisions as well as merger-and-acquisition processes; encourage collaboration with stakeholders and peers; and provide CISOs with a degree of protection when inevitable risks occur. These broad recommendations can be categorized as follows:



1. PROCUREMENT AND RISK MANAGEMENT

a. Shared Procurement and Business Transformation Responsibility

CISOs should have the authority to work with all relevant business unit leaders (from Legal to Government Affairs to Privacy to Human Resources) to establish formal points of integration in the strategic planning, design, build, and purchase processes. These touchpoints may be tied to, for instance, new business ventures or technology acquisitions. This way, an organization can weigh security considerations well before it acquires new assets or business operations, or implements new tools that create risks the CISO would be responsible for responding to should they materialize.

i. Mergers and Acquisitions (M&A).
Organizations should consider cybersecurity risks during the due diligence phase of M&A activities. The CISO should be an integral part of this risk assessment process. If the CISO does not participate in M&A activities, the organization is unlikely to understand the full risk of acquisition and the full cost of integration.

b. Budget Authority

CISOs should have budget authority over the assets and processes that directly impact information security systems and oversight to ensure that security is considered throughout the lifecycle of a system.

c. Protection for Risk of Personal Liability

Because CISOs can be subject to personal liability, businesses should provide protection, including considering whether it is possible for their CISO to receive coverage under a directors & officers insurance policy, and include them as part of the coverage where possible.

d. Enterprise Risk Management

Because cyber security risks permeate the business and are not just technology risks, the CISO should have access to and influence across the various risks associated with cybersecurity. As a result, when necessary, and in partnership with peer business units, CISOs should have the power to make and enforce enterprise-wide security decisions.

2. HORIZONTAL AND VERTICAL INTEGRATION OF CISOS

Because there are risks that an organization creates throughout its entire enterprise, CISOs and their functional equivalents should be integrated at key decision-making junctures internally. This integration should include at least the following categories:

a. Peer Business Units

CISOs and leaders of other business units should have strong partnerships.[5] For example, CISOs and Human Resources or Legal functions should work together to incorporate user-level security responsibilities embedded in employee policies. CISOs should have especially close relationships with an organization's technology departments, as the CISO must work closely with the CIO, the CTO, and other technology leaders, including lead architects, to ensure cybersecurity is considered as part of all technology-related decisions. The alignment of the CISO function to the other profit-and-loss functions and entities is similarly important.

b. Boards and CISOs

Organizations should consider creating a technology and cybersecurity committee on their board of directors, or equivalent, that includes quarterly updates from the CISO or IT security function. The technology and cybersecurity committee chair should in turn report updates to the full board.

5. As an example, CISOs are increasingly required to implement compliance certification programs, and then to attest to these certifications (e.g., PCI-DSS, SOC 2, FedRamp, etc.). The successful completion of these processes requires close relationships with peer corporate functions, such as the Office of the Controller, Federal Sales, and Data Privacy teams.

c. Reporting Structure

CISOs must have direct and meaningful access to key decision-makers in the C-suite. This also means CISOs should have the ability to raise serious security concerns to leadership without concern for personal consequences. The precise structure can vary from organization to organization, but it is critical that the CISO have access to and accountability from an individual with institutional decision-making power, such as a general counsel, CTO, CFO, or CEO.[6] In addition, the CISO should be a standing member of the corporate compliance and corporate disclosure committees.

CONCLUSION

Years ago, many saw the CFO as a technical advisor to the C-Suite—the CFO managed updates to a company's books and records in order to comply with a variety of regulations, but, otherwise, organizations did not fully integrate CFOs into the organizational decision-making process. That work was for the strategic executives. And then, as the business and regulatory environment evolved, things changed. CISOs are experiencing a similar shift. The typical CISO operates in a fundamentally changed terrain, and it is time for organizations to adjust accordingly.

6. Regardless of the CISO's specific reporting structure, institutions must assess the scale of business functions and processes that require cyber governance as they determine the appropriate scope of CISO authorities and, by extension, the reporting structure. In this evaluation, organizations should consider including product security as a CISO function, which could be part of a successful operating model for CISOs. This new structure should also be accompanied by appropriate funding and oversight.