

# Elevating Cybersecurity: Ensuring Strategic and Sustainable Impact for CISOs

WHITE PAPER  
OCTOBER 2025



# Contents

Foreword	3
Executive summary	4
Introduction	5
1 The complexity surrounding the CISO role	6
1.1 The intricate landscape in which the CISO operates	6
1.2 The diversity of the CISO role	8
2 Recommendations for CISOs and top leadership	17
2.1 The evolving responsibilities of the CISO	17
2.2 What can CISOs do to make the case for cybersecurity as a business imperative?	18
2.3 What can boards do to empower CISOs?	19
Conclusion	20
Contributors	21
Acknowledgements	21
Endnotes	25

## Disclaimer

This document is published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

© 2025 World Economic Forum. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

# Foreword



**Christophe Blassiau**

Senior Vice-President  
and Group Chief Information  
Security Officer, Schneider Electric;  
Co-Chair, World Economic Forum  
CISO Community



**Sabrina Feng**

Chief Risk Officer, Technology,  
Cyber and Resilience, London  
Stock Exchange Group (LSEG);  
Co-Chair, World Economic  
Forum CISO Community



**Akshay Joshi**

Head, Centre for  
Cybersecurity, Member of  
the Executive Committee,  
World Economic Forum

In today's digitally interdependent world, the role of the chief information security officer (CISO) is more critical and complex than ever. Security leaders must navigate geopolitical volatility, technological disruption and systemic cyber risks, all while building trust and driving innovation.

Cybersecurity is now a core business imperative. The CISO's remit extends far beyond technical defence: it involves translating global shifts into actionable strategies, guiding the secure adoption of emerging technologies – such as AI and quantum computing – and building resilient ecosystems with partners, regulators and peers. To succeed, CISOs need more than responsibility and credibility – they need systemic empowerment. Boards and executives must recognize that the CISO role needs a broad mandate.

This white paper, shaped by the World Economic Forum's global CISO community and grounded in real-world experience, offers a practical view on elevating cybersecurity within an organization through the analysis of the CISO role. It highlights how organizations can transform cyber risk into resilience and convert trust into sustainable value creation.

We urge every leader – whether in the boardroom, the C-suite or the security team – to seize this moment. By redefining the CISO as a strategic enabler, cybersecurity can evolve from a cost centre or compliance exercise into a driver of growth, trust and innovation.

# Executive summary

The chief information security officer has become central to the success of the business. Boards and C-suite executives can actively contribute to making cybersecurity a strategic imperative within the organization.

As organizations confront a rapidly evolving and interconnected threat landscape – especially from organized criminal groups and state-sponsored cyber operations, AI-enabled attacks and supply chain vulnerabilities – the role of the CISO is undergoing a profound transformation. Today's CISO must act as a business strategist, operational risk leader and trusted adviser to executive leadership and boards.

The shift towards positioning cybersecurity as a core business risk has accelerated in recent years. Regulatory frameworks now frequently mandate the appointment of a CISO and define their accountability structures.<sup>1</sup> At the same time, the consequences of cyber incidents – such as operational disruption, reputational damage and erosion of customer trust – have become more visible and severe. However, in the [Global Cybersecurity Outlook 2025](#) survey, almost twice as many surveyed CISOs than CEOs identified brand damage and loss of customer trust as their top concerns amid geopolitical tensions. This gap highlights a continued misalignment at the executive level regarding cyber risk prioritization.

Drawing on insights and engagements with CISOs in the World Economic Forum's CISO community, this white paper discusses how the position is expanding in scope and influence amid the growing complexity of the cyber landscape, and outlines the key roles CISOs must fulfil to position themselves as strategic enablers.

Boards have a role to play in empowering the CISO to exercise effective leadership and deliver strategic and sustainable impact. The success of the CISO depends on influence rather than hierarchy. To do this, boards must empower CISOs with a clear, enterprise-wide mandate that recognizes cybersecurity as a fundamental enabler of resilience, trust and long-term value. This white paper also addresses boards and provides them with a set of enablers that help elevate cybersecurity within the organization so that the CISO can develop trusted relationships in both internal and external ecosystems – spanning the C-suite, risk and compliance functions, operational units and government bodies. Elevating cybersecurity is also about strengthening the organization's overall resilience.



# Introduction

In 2025, with the global cyber landscape both fragmenting and becoming more deeply interconnected, the role of the CISO stands at a defining crossroads.

The transformation of the cyber landscape has critical implications for how the CISO operates and sets the cybersecurity strategy in relation to broader business priorities.

The shift from information security to cybersecurity reflects a move from protecting classified information – rooted in military and government cryptographic efforts – to safeguarding the wider use of digital technologies. Early computing was primarily focused on encrypting, decrypting and securing information for government use. As computing expanded into civilian and industrial domains, the threat landscape became more diverse, leading to a more holistic approach to cybersecurity.

When it emerged, the CISO role focused primarily on the technical aspects of information security: ensuring the protection of information technology (IT) infrastructure by overseeing firewalls, intrusion detection systems and incident response protocols. The role was often siloed, sometimes within, or sometimes separate from, the IT department, with limited visibility at the executive level. Today, however, this legacy model is no longer sufficient. The scope and strategic relevance of cybersecurity have expanded dramatically, bringing the CISO role into sharper focus across the enterprise.

As highlighted in the *Global Cybersecurity Outlook 2025*, a range of external pressures are reshaping the expectations placed on CISOs, from intensifying geopolitical tensions to the rise of cybercriminal syndicates, as well as a fragmented regulatory environment and emerging technologies such as AI and quantum computing. These dynamics demand that security leaders not only manage risk but also guide organizations through uncertainty, act as strategic advisers and foster trust within and beyond the enterprise.

This white paper explores the evolution of the CISO role in the face of rising complexity, outlining how this complexity manifests, what it demands of today's cybersecurity leaders and how the structure of the CISO role – along with its relationships and reporting lines – must adapt. It provides a clear mapping of the CISO's interactions with principal stakeholders, offering a practical view to help boards and CISOs align cybersecurity strategy with organizational resilience, business growth and board expectations.

# The complexity surrounding the CISO role

The increasing complexity of the cyber landscape is reshaping the role of the CISO.

## 1.1 The intricate landscape in which the CISO operates

The transformation of the cyber landscape calls for dialogue between practitioners and business leaders to redefine the fundamental attributes of the CISO.<sup>2</sup> Before examining this in more detail, this paper explores how each of these factors of complexity – and their interplay – affects and shapes the CISO role and mandate.

- **Geopolitics:** Geopolitical tensions exert an influence on cyber strategy in nearly 60% of organizations, according to the *Global Cybersecurity Outlook 2025* survey. In addition, the *Microsoft Digital Defense Report 2024* emphasizes the escalation of state-sponsored cyberthreats.<sup>3</sup> Current geopolitical tensions – which can lead to wars or tariffs – require CISOs to adapt their security strategy and advise the business on their approach to security towards different events, such as changing regulations, technologies under sanctions, reputational damage and so forth. The current debates on data sovereignty, driven by the shifting geopolitical landscape, are also influencing countries' and organizations' technology narratives. As systems become increasingly fragmented regionally, it makes it harder for CISOs to aggregate data to detect attacks. CISOs need to find efficient ways to gain central visibility over a more diverse and dynamic systems landscape.
- **Cybercrime:** Some 72% of respondents to the *Global Cybersecurity Outlook 2025* survey said that cyber risks have risen in the past year. Some of the factors may include the rise of cyber-enabled fraud, driven by an increase in phishing and social engineering attacks. Additionally, identity theft is one of the top risks that concerns people on an individual level. The increased volume of cybercriminal networks and cybercrime types – including advanced persistent threats (APTs) developed by state-sponsored groups, scam farms, ransomware and supply chain attacks – means that CISOs need to proactively determine how to make threat intelligence actionable and valuable for their organizations and focus on establishing trusted collaboration lines with peers within their ecosystem.
- **Regulatory requirements:** According to the *Global Cybersecurity Outlook 2025* survey a total of 78% of leaders from private organizations feel that cyber and privacy regulations effectively reduce risk in their organization's ecosystems. However, the complexity and proliferation of regulatory requirements poses a significant challenge. Geopolitical tensions and emerging technologies, among other factors, have led to diverging regulations across regions. The cybersecurity compliance landscape thus becomes more fragmented, adding layers of compliance levels. CISOs need to devote more resources to managing a higher number of (sometimes opposing) requirements.
- **Emerging technologies:** Some 66% of respondents to the *Global Cybersecurity Outlook 2025* survey believe that AI will affect cybersecurity in the next 12 months, but only 37% have processes in place for safe AI deployment.<sup>4</sup> Additionally, AI-related spending across industries is projected to reach approximately \$639 billion by 2028.<sup>5</sup> The rise of digitalization and innovation – with the development of technologies such as quantum computing – expands the attack surface that CISOs manage, while rapidly evolving technologies demand that CISOs and their teams stay continuously informed about both the associated risks and the potential benefits to the business. CISOs need to balance the speed of innovation while adapting quickly to ensure the resilience of their organizations.

- **Supply chains:** With more than half of large organizations citing third-party risk management as a major challenge, supply chain challenges remain a top concern for achieving cyber resilience.<sup>6</sup> The growing interdependencies of (digital) supply chains imply that cyberthreats can come from a multitude of entry points. Additionally, as integral players in their clients' supply chains, organizations have a responsibility to uphold strong cybersecurity practices across both upstream and downstream interactions – protecting not only supplier connections but also customer relationships.<sup>7</sup> CISOs must foster collaborative security, make sure there are no blind spots among their suppliers and develop strong relationships with the most critical of these to ensure resilience in the event of a percolating cyber incident.
- **The cyber skills gap:** The cyber skills gap has widened since 2024, with two in three organizations reporting moderate-to-critical skills gaps. In today's hyperconnected digital landscape, the cybersecurity industry faces a critical global shortage, with estimates ranging from 2.8 million to 4.8 million unfilled positions.<sup>8,9</sup> Research shows that the cybersecurity skills shortage creates additional cyber risks for 70% of organizations.<sup>10</sup> Additionally, ISACA's *State of Cybersecurity 2024* report notes rising stress levels among cybersecurity professionals due to increased workloads and complex threat environments.<sup>11</sup> The current cybersecurity talent pool is still under-developed and insufficient to meet workforce demand. CISOs must build teams that are attractive to talent, nurture that talent internally, ensure the well-being of their employees and use technology innovatively to augment the capacity of their teams.
- **Constant emergence of new vulnerabilities:** This creates a persistent and worsening dilemma – while business pressures demand speed and innovation, security remediation adds requirements and time to technology deployment. The gap between security needs

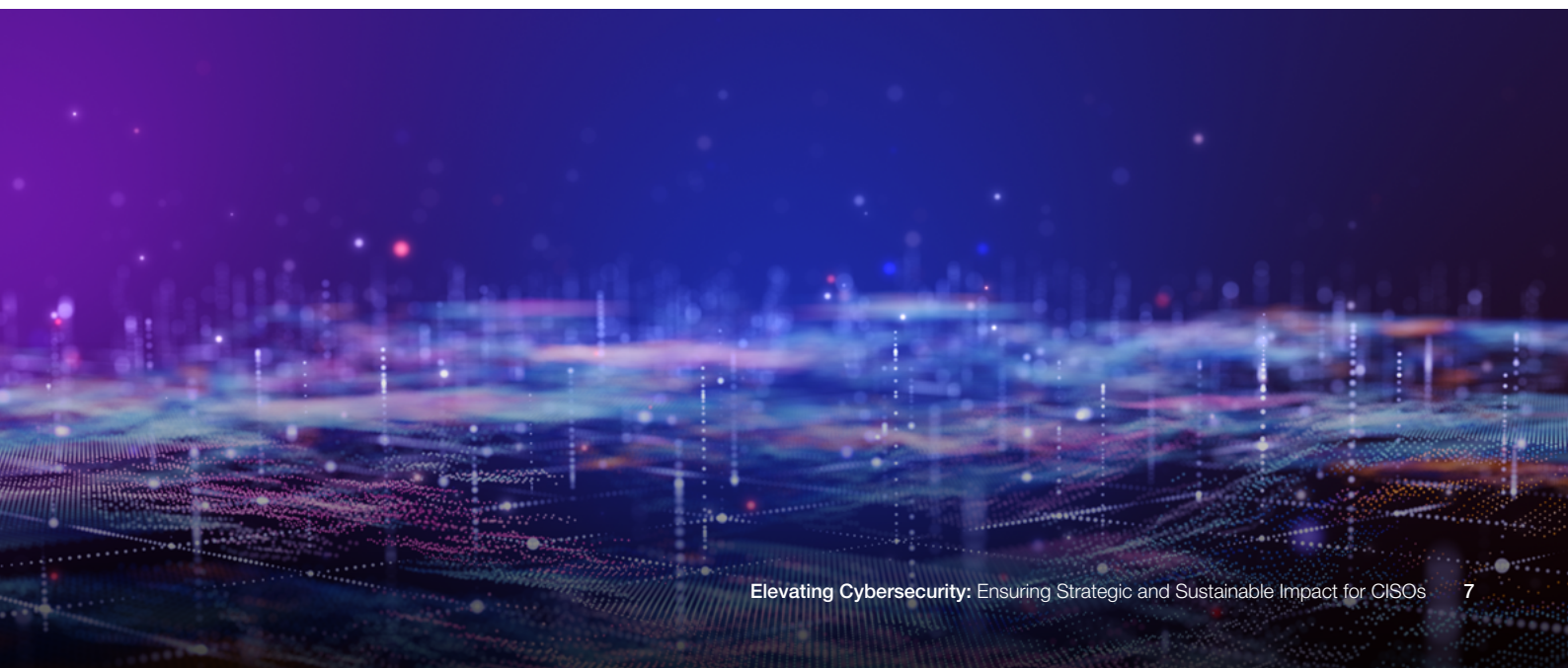
and actual implementation continues to widen, making organizations more susceptible to breaches. Accelerated action from CISOs on security measures is no longer optional; it is essential to maintaining resilience in an increasingly hostile digital landscape.

- **The ever-changing risk landscape:** Change is constant in modern organizations – whether through technology upgrades, configuration tweaks or daily code deployments. However, this velocity of change heightens cyber risk. Security gaps are often unknowingly introduced by business teams who may not fully grasp the downstream security implications. Meanwhile, new application code is pushed rapidly into production, in some instances without the knowledge or involvement of the CISO or security teams. This lack of visibility and control creates blind spots and a risk of unanticipated security exposures. CISOs must invest time and effort to keep oversight across the full digital footprint of the enterprise.

Taken together, these factors illustrate the increasingly complex environment in which CISOs are expected to operate. Additionally, while CISOs are accountable for protecting the organization from cyberthreats, they often do not control all IT or OT (operational technology) systems. Therefore, establishing and maintaining an influence over business unit decisions or vendor selections becomes paramount.

The CISO role is thus evolving beyond its traditional technical boundaries to encompass a more strategic, collaborative function within the organization. To remain effective, CISOs must engage across business lines, stay aligned with regulatory and technological developments and ensure that cybersecurity supports overall organizational resilience and decision-making.

In this context, there is a growing need to explore the CISO mandate, relationships, tools and culture to ensure that CISOs are equipped to respond to both present and future challenges.



## 1.2 The diversity of the CISO role

### A. The CISO mandate

There is no single definition of a CISO. The exact title and mandate depend on a variety of factors such as the size of the organization, its industry, its age, its market segment and its cyber maturity.

In some organizations, roles and responsibilities with regard to risk governance are defined through the “three lines of defence model”. In this, used widely in the financial services industry, responsibilities are split among: the first line of defence, which runs operations to protect the organization against cyberthreats; the second line, focusing on risk management and compliance; and the third line, delivering internal auditing. Some CISOs may sit in the first or second line, while others operate across both lines. Some CISOs focus narrowly on specific parts of the business, while others have a broader, more holistic scope encompassing all digital systems, including the product or service offering from their organization, therefore protecting the value proposition delivered to clients. Reporting lines may also vary, with some CISOs reporting to a member of the C-suite – for example, the chief information officer, chief technology officer, chief legal officer, chief risk officer or chief digital officer – while others report directly to the chief executive officer. At the World Economic Forum’s Annual Meeting on Cybersecurity 2024, 24% of CISOs polled had direct reporting lines to the chief executive officer.

Some organizations integrate physical security and personnel security as part of the CISO role, while others include crisis management and business continuity – this often results in a wider chief security officer (CSO) role with the intention of aligning those mandates. CISOs’ remit may now include hybrid, physical and human capital risks (and more). Some financial services organizations also broaden the scope of the CSO role to include financial crime, anti-fraud and anti-money laundering, making their scope wider than

traditional information security. Some CISOs own identity, while other organizations keep it separate.<sup>12</sup> Some other CISOs may also own the trust or resilience agendas. For organizations operating in industrial ecosystems, the CISO often has the responsibility of ensuring the digital security of OT.

In some cases, the C-suite looks at the CISO role as being compliance-driven, which can be a limiting framework if the aspiration is to build a cyber-resilient organization. Compliance is about meeting minimum standards; security is about managing real-world risk. Therefore, the balance between compliance and security is crucial to the CISO role.

Globally, cybersecurity is increasingly recognized as a core element of corporate governance and board-level accountability, driven by regulatory developments across multiple jurisdictions. Laws and frameworks emphasize that boards of directors bear ultimate responsibility for managing cyber risk. While operational duties may be delegated to a CISO, the legal and reputational consequences of cybersecurity failures remain with the board – making the CISO’s primary role one of enabling the board to fulfil its fiduciary, legal and risk management obligations. Although CISOs must work closely with business units to implement effective controls and drive resilience, one of their core values lies in enabling the board and executive leadership by providing strategic insight, assurance and clear communication of the organization’s cybersecurity posture.

### B. CISO relationships

CISOs’ success hinges on strong relationships to enable tactical and strategic collaboration across their organization and beyond. Figure 1 shows a map of the CISO relationships and outlines the key stakeholders and high-level responsibilities from both sides.

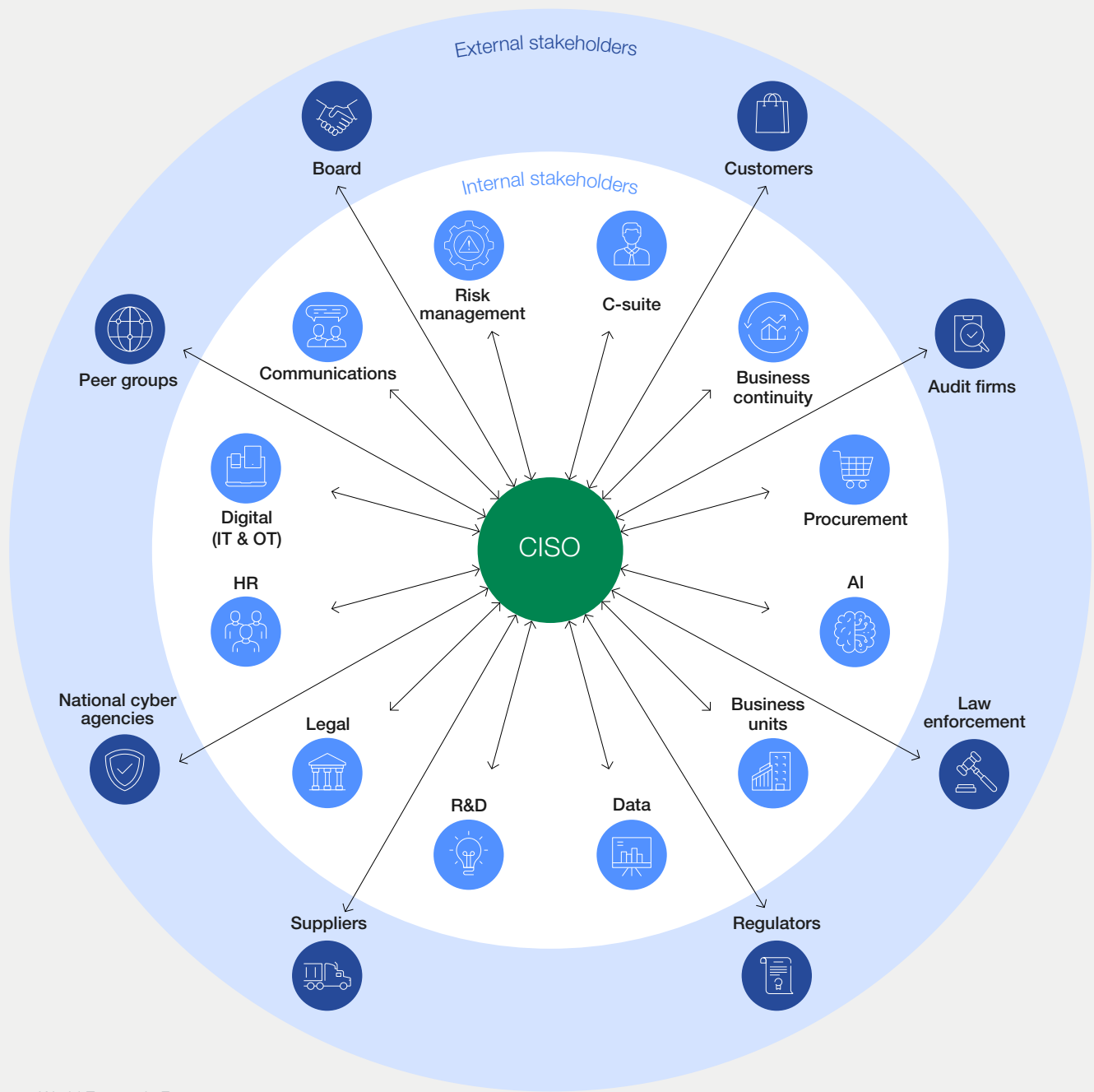


**In today’s rapidly evolving threat landscape, the role of the CISO has never been more critical. CISOs are not just defenders of infrastructure – they are strategic leaders who work across every part of the organization to embed security into the fabric of how an organization operates, innovates and serves customers. At PayPal, the most critical responsibilities of the CISO are to align security with business priorities, foster a culture of trust, drive resilience at scale and protect the company and its customers.**

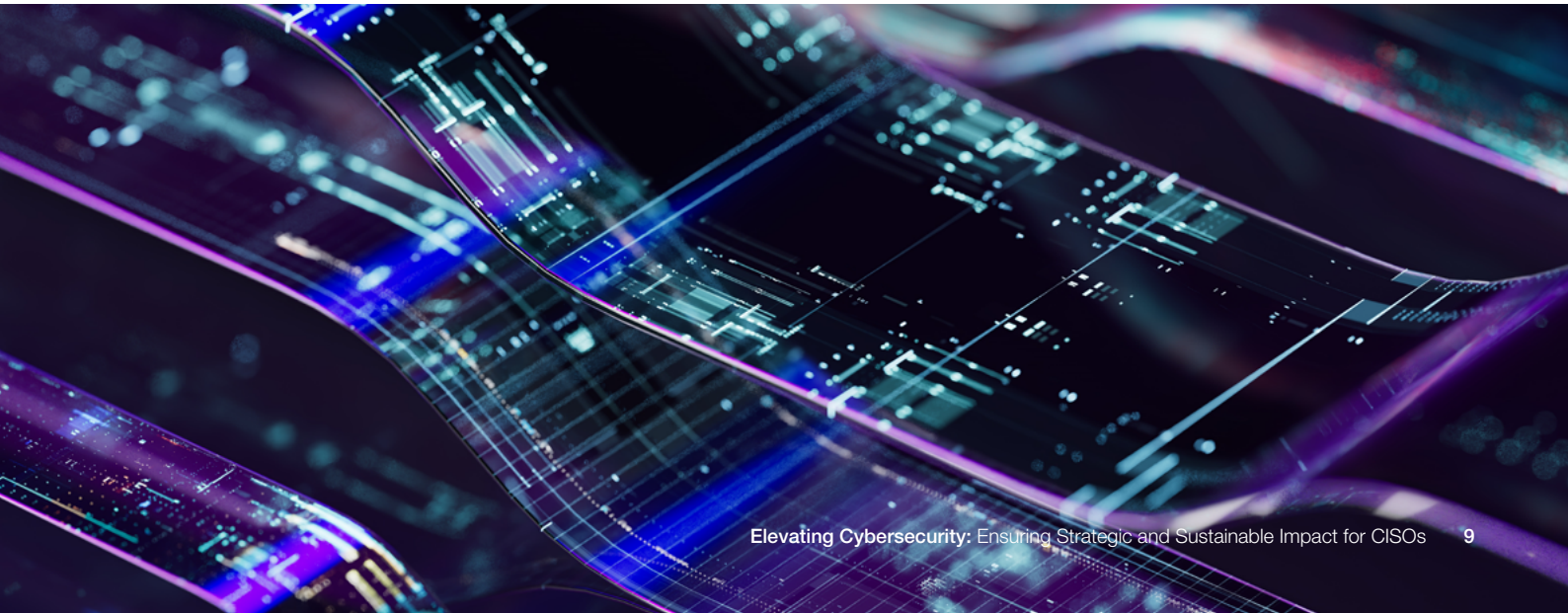
Joy Chik, Board Member at PayPal



FIGURE 1 | The CISO's strategic collaboration network



Source: World Economic Forum



## High-level relationships

### External stakeholders



#### Board<sup>13</sup>

##### Responsibilities of the CISO to the board

- Raise awareness and educate on cyber risk with regard to business strategies and decisions
- Provide a clear narrative on the cybersecurity posture of the organization in the longer term
- Present cyber risk in terms of business impact, financial exposure, regulatory implications and reputational risks

##### Responsibilities of the board to the CISO

- Ensure the CISO has the resources, budget and team needed to secure the organization
- Work closely with the CISO to encourage systemic resilience and collaboration throughout the organization
- Design an organizational structure that supports cybersecurity
- Align cyber-risk management with business needs



#### Customers

##### Responsibilities of the CISO to customers

- Provide transparency on key cybersecurity activities and posture (for example, in the annual report)
- Develop a trusted relationship and open a communication channel in case of an incident

- Partner with customers to deliver solutions that meet the customer's risk tolerance as well as regulatory requirements

##### Responsibilities of customers to the CISO

- Communicate incidents in a timely manner



#### Suppliers

##### Responsibilities of the CISO to suppliers

- Clearly communicate how critical the supplier is to the security of the CISO's organization
- Communicate new vulnerabilities in a timely manner

- Develop a trusted relationship and open a communication channel in case of an incident

##### Responsibilities of suppliers to the CISO

- Provide timely communication on incidents and share any compromise-related information



#### Law enforcement

##### Responsibilities of the CISO to law enforcement

- Build a collective defence and strong collaboration lines to share information that helps law enforcement activities if required

##### Responsibilities of law enforcement to the CISO

- Provide relevant intelligence to help improve the organization's preparedness



## National cybersecurity agencies and incident response centres

### Responsibilities of the CISO to cybersecurity agencies and incident response centres

- Share intelligence on vulnerabilities and threats that are intercepted
- Develop a trusted relationship and open a communication channel in case of an incident

### Responsibilities of cybersecurity agencies and incident response centres to the CISO

- Consult the organizations and industry when developing guidance and frameworks for cybersecurity
- Issue pragmatic cybersecurity frameworks, policies and guidelines to help businesses adopt robust security measures
- Assist the organization in mitigating and recovering from cyber incidents through coordination, technical support and forensic analysis



## Regulatory/standards bodies

### Responsibilities of the CISO to regulatory/standards bodies

- Develop a trusted relationship and open a communication channel in case of an incident

### Responsibilities of regulatory/standards bodies to the CISO

- Set and enforce cybersecurity regulations (for example, data protection laws, sector-specific requirements)
- Oversee private-sector cybersecurity practices to reduce risk and protect consumers



## Audit firms

### Responsibilities of the CISO to audit firms

- Present a clear and transparent overview of the organization's cybersecurity strategy, governance model and control framework
- Provide an accurate overview of risks, incidents or control weaknesses

### Responsibilities of audit firms to the CISO

- Evaluate the effectiveness of the organization's information security controls, policies and procedures and provide unbiased insights into risks
- Provide assurance to external and internal stakeholders (for example, regulators, board, customers) that the CISO's security function is effective and trustworthy



## Cybersecurity peer groups

### Responsibilities of the CISO to cybersecurity peer groups

- Participate in the community by sharing best practices and threat intelligence

### Responsibilities of cybersecurity peer groups to the CISO

- Provide support and mentoring as well as share useful practices (for example, benchmarking on security programmes, incident response plans templates and so forth)

## Internal stakeholders



### C-suite and key allies (top leadership, such as chief financial officers, chief risk officers, chief digital officers, chief legal officers, chief information officers)

#### Responsibilities of the CISO to C-suite and key allies

- Align cyber strategy with business objectives and collaborate with C-suite members to ensure cybersecurity supports the company's growth and resilience
- Ensure alignment with business needs to provide a strong case for cybersecurity activities within the organization
- Provide a clear view on the cyber posture of the organization with regard to its overall risk tolerance and appetite; regularly report

on the status of the cyber posture, including advances, issues and resourcing needs

#### Responsibilities of C-suite and key allies to the CISO

- Ensure the CISO is well equipped financially to protect the organization and that they are empowered to establish key relationships within the organization
- Undertake training on cybersecurity, including in collaboration on cyber incident response



### Risk management and compliance teams

#### Responsibilities of the CISO to risk management and compliance teams

- Communicate cyber risks and related mitigating actions
- Consult and seek advice on how to align cyber risks with overall risk appetite and tolerance

#### Responsibilities of risk management and compliance teams to the CISO

- Steer the reporting of cyber risks into enterprise risks so that they are treated as part of the organization's overall risk profile
- Assist in managing vendor risks
- Disseminate cyber-related regulatory requirements to relevant (non-tech) audiences internally



### Digital (IT & OT) teams

#### Responsibilities of the CISO to digital teams

- Develop a partnership and collaborative relationship with an open communication line
- Provide policies, standards and guidance for secure and resilient implementation, use and decommissioning of key technology components

#### Responsibilities of digital teams to the CISO

- Communicate and report on the technological evolution and implementation of key technologies
- Consult and follow cybersecurity advice and requirements



### AI teams

#### Responsibilities of the CISO to AI teams

- Learn about new applications and uses of AI within the enterprise
- Provide cyber-related advice in a timely manner, taking into consideration the business requirements, and expand traditional app-security reviews, for example, to include ethics, bias, model security and prompt analysis

#### Responsibilities of AI teams to the CISO

- Involve and consult the cybersecurity team early in the development of new products and services to make sure cybersecurity practices are embedded from the outset





## Data teams

### Responsibilities of the CISO to data teams

- Conduct regular risk assessments focused on data-related assets and processes

### Responsibilities of data teams to the CISO

- Promptly report any suspected or actual data breaches, leaks or anomalies to the CISO or security operations team
- Implement safeguards that help withstand business disruptions and ensure the availability of services



## Procurement teams

### Responsibilities of the CISO to procurement teams

- Provide guidance on key criteria to assess third parties and suppliers
- Offer guidance to enhance general terms and conditions with cybersecurity-related

requirement and associated oversight of third parties and suppliers

### Responsibilities of procurement teams to the CISO

- Provide visibility into the business criticality of third parties and suppliers



## Research and development (R&D) teams

### Responsibilities of the CISO to R&D teams

- Provide advice in a timely manner, taking into consideration business requirements

### Responsibilities of R&D teams to the CISO

- Involve and consult the cybersecurity team early in the development of new products and services to make sure cybersecurity practices are embedded from the outset



## Legal teams

### Responsibilities of the CISO to legal teams

- Consult on a regular basis and when a change of regulation occurs in order to understand any impact on cybersecurity practices

### Responsibilities of legal teams to the CISO

- Communicate new cyber-related requirements in a timely manner and help the CISO translate the requirements into business terms



## Business continuity teams

### Responsibilities of the CISO to business continuity teams

- Closely align cyber resilience plans with the central business continuity and crisis management processes

### Responsibilities of business continuity teams to the CISO

- Communicate crises in a timely manner when they may have a ripple effect on cybersecurity and cyber resilience



## Communication teams

### Responsibilities of the CISO to communication teams

- Provide accurate, timely and contextual information about security risks and incidents to enable clear, trustworthy messaging

### Responsibilities of communication teams to the CISO

- Provide the CISO with clear, timely and strategic messaging support and mechanisms to ensure consistent internal and external narratives during both routine operations and security incidents



## HR teams

### Responsibilities of the CISO to HR teams

- Provide clear security policies, risk awareness guidance and timely updates on employee-related threats to help enforce compliance and promote a secure organizational culture

### Responsibilities of HR teams to the CISO

- Provide the CISO with up-to-date employee data, support for enforcing security policies and collaboration on training programmes to strengthen the organization's security awareness and compliance culture



## Internal business units and employees

### Responsibilities of the CISO to internal business units and employees

- Raise awareness of the cyber risks and the role each employee plays in the security and resilience of the business
- Build a trusted relationship with open lines of communication

### Responsibilities of internal business units and employees to the CISO

- Consult on a regular basis and follow guidance provided
- Report incidents in a timely manner



## SPOTLIGHT

## The board as a cyber ally, not an examiner

Most CISOs from the World Economic Forum's CISO community report interacting with their board on a regular basis, many quarterly. Regular, proactive engagement with the board is essential. CISOs should feel that they can ask boards for help or advice, as it is a collaborative relationship. Although first board meetings may feel like an exam to CISOs, the board members' intention is not to test the CISO but rather to understand the full picture and share their experience on what is presented to them.

Regarding corporate governance on cybersecurity matters, some organizations have set up a security committee midway through the quarter to get additional time to focus on cybersecurity issues outside of board meetings. Other companies run a dedicated subcommittee of the board with a focus on cybersecurity risk. Those security committees can help maintain focus on cybersecurity and continuity in dealing with it.

A key to success is to raise the risks and challenges with the board before any potential threats become real issues, so there are no surprises if an incident arises. Qualitative metrics can help tell a story and demonstrate impact better than quantitative ones can. To prepare, CISOs should consult previous board reports to glean historical information on how cybersecurity has been discussed and addressed by the organization in the past.

CISOs should create their own equivalent of a Richter scale: a mechanism for understanding and reflecting the degree of criticality from a scenario or a risk. It could also help boards prioritize what to focus on and what to ignore, parsing the signal from the noise and knowing when to become more closely involved.



**Successful CISOs proactively engage with the board, providing regular updates and insights on the evolving risk environment along with actionable recommendations. They understand that effective cyber risk management is not an isolated function, but one that must be integrated and synchronized with key areas like privacy, government relations, operations and sales to protect customers and the company.**

Laura Quatela, Non-Executive Director, Board of Directors, Lenovo



### C. CISO tooling

One of the challenges CISOs consistently face is tooling complexity.<sup>14</sup> The cybersecurity market is highly fragmented, and security teams often manage dozens of tools that do not fully integrate. This leads to inefficiencies, alert fatigue and increased overheads. CISOs also sit on large volumes of security and business data, which is a potential enabler for smarter automation and process improvement. As the function matures, effective tooling strategies should focus on simplification, interoperability and measurable value to the enterprise.

- **Use emerging technologies for security, efficiency and enhancing the cyber team's skills:** To stay ahead of cyberattackers, CISOs should strategize how emerging technologies can enhance their operations and streamline the vast amount of security tooling that is in place.
- **Exercise budget discipline:** A zero-based budgeting approach should be applied to cybersecurity tooling – regularly reviewing the portfolio and eliminating underused or ineffective tools.
- **Be metric-driven:** CISOs should make the best use of tooling to understand how the technology works, define what they want to measure and collect data that will support their assessment of the technology. From this data – for example, mean time to detect (MTTD), mean time to respond (MTTR) and so forth – they can determine the cybersecurity posture of their organization.

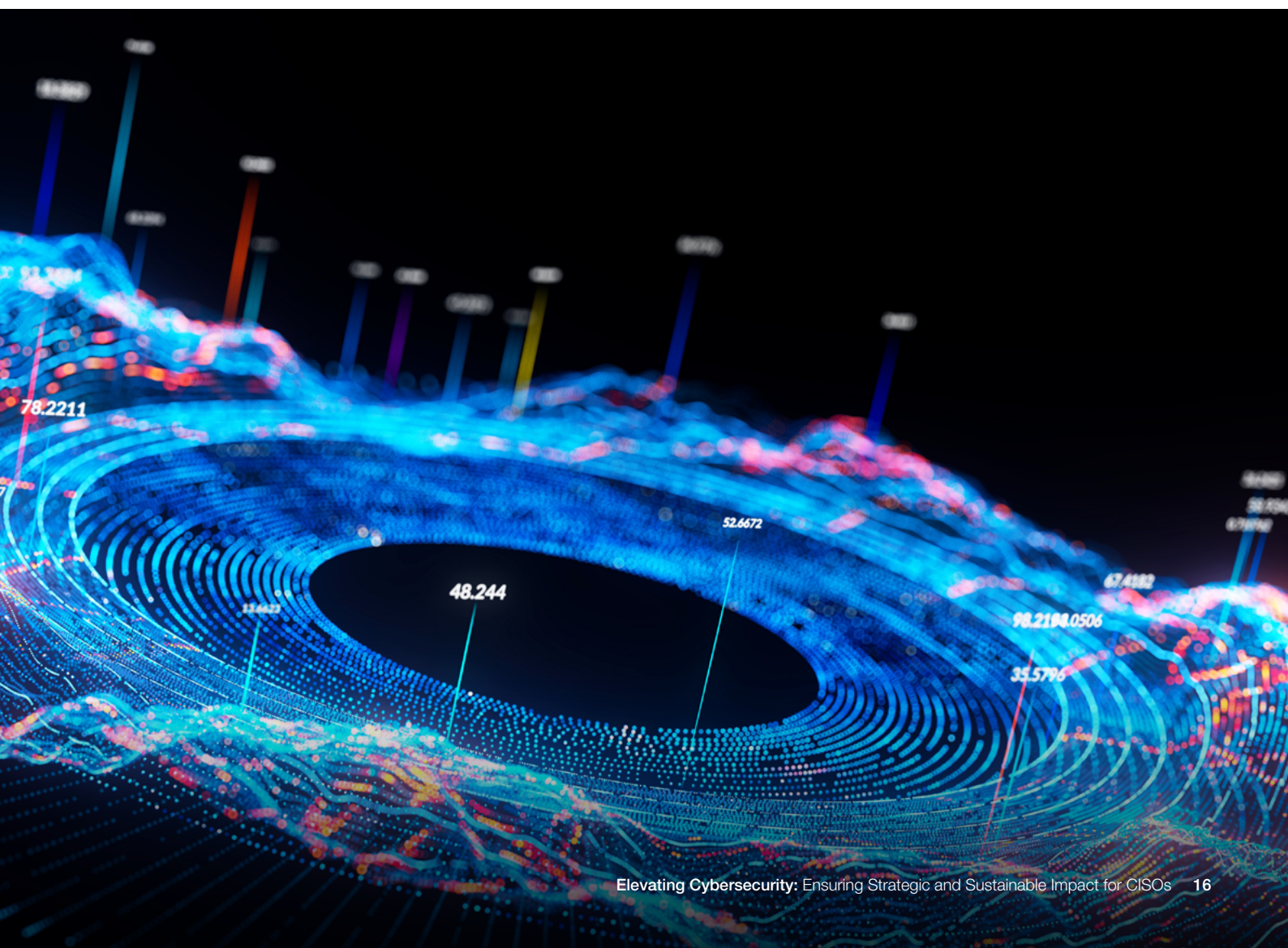
- **Act as an adviser and rationalizer:** As organizations constantly update their current tooling to stay ahead of technological shifts and developments, instead of pursuing “rip and replace” strategies, CISOs should simplify and rationalize tooling, acting both as an internal adviser and a discerning customer, thus managing complexity at scale.
- **Operate with agility and integration:** Agility with technology is essential as CISOs must collaborate closely with the business, engaging at the point of need rather than imposing constraints. An agile mindset should not, however, lead to compromises on basic cyber hygiene and on clarity and accuracy in the face of a cyber incident.
- **Implement standardized reporting:** CISOs can develop third-party toolkits that bring consistent approaches to penetration testing for tools that are critical to the organization – this can greatly support the compliance effort.

### D. CISO mindset and culture

A strong cybersecurity mindset and culture are foundational to an organization's ability to defend against cyberthreats. The cybersecurity culture reflects the collective awareness, behaviours and attitudes of employees towards protecting their own organization. When security becomes an integral part of daily decision-making – from executive strategy to individual actions – organizations are better equipped to prevent breaches, respond to incidents and build long-term resilience.



- In many places, the organizational cybersecurity culture is still focused on a preventative and protective approach. Given the unpredictability of the cyber landscape and the multitude of potential vulnerabilities, there is a need to add cyber resilience as a core focus – a strong case for evolution towards a mindset that encompasses detection and response, including scenario analysis on the impact and evolution of cyberthreats.
- Cybersecurity must be positioned as a business enabler rather than a barrier, encouraging CISOs to embrace a “Yes, and ...” mindset. To achieve this, CISOs should prioritize a deep understanding of business objectives and align security initiatives accordingly. Crucially, they must translate technical risks into clear business risks, enabling informed decision-making at the executive level.
- The highest level of cybersecurity maturity is achieved when employees without technical expertise understand the need for the cybersecurity controls that are in place and do not see them as undue restrictions. This reflects a culture of shared responsibility and open dialogue. Organizations that position cybersecurity as an enabler of business growth – enhancing operations, resilience and reputation – tend to demonstrate greater overall resilience.<sup>15</sup>
- The risk culture should be embedded into all layers and across all teams within an organization. Risk ownership must be shared across the business, with decision-makers understanding and accepting the residual risk, acknowledging that the CISO cannot mitigate them all.
- CISOs should foster a culture that encourages proactive testing of systems, where the discovery of new vulnerabilities is viewed as an opportunity to strengthen security rather than as a failure. For example, red teaming exercises – simulated cyberattacks conducted by ethical hackers – might uncover hidden vulnerabilities and blind spots that traditional security assessments can overlook. This proactive approach provides invaluable insights into how threat actors could breach systems, allowing security leaders to prioritize fixes before actual incidents occur.
- A long-term mindset is also paramount as CISOs are required to “play the long game”. This means making a long-term commitment to improving cyber maturity and implementing sustainable practices that will allow an organization to reach its security targets. Acknowledging that 100% risk reduction cannot be achieved, a long-term roadmap that targets sustainable cybersecurity maturity improvement is required.





# Recommendations for CISOs and top leadership

A CISO's relationship with the C-suite and board is critical to positioning cybersecurity as a powerful enabler of business growth and resilience.

## 2.1 The evolving responsibilities of the CISO

The role of the CISO is increasingly seen as a launchpad for broader executive leadership. While some CISOs may remain in the role long-term, others are transitioning into positions such as chief security officer (CSO) or chief risk officer (CRO), with expanded mandates covering physical security, enterprise risk, operational resilience and organizational trust.

This evolution is in response to an expanding and converging risk landscape. CISOs are uniquely equipped to navigate complex, ambiguous threats, from misinformation and geopolitical disruptions to infrastructural failures, even when these risks fall outside traditional cybersecurity domains. Their expertise in systemic risk management often positions them as key figures in crisis response and organizational resilience.

At the same time, the CISO's role in evaluating and securing emerging technologies is becoming more critical. As innovations such as generative AI and quantum computing get embedded into core operations, CISOs must anticipate new threat models, ensure responsible deployment and align security controls with business innovation goals.

As a result, CISOs' scope often starts to assume broader responsibility within the organization for enterprise security, trust and resilience. In addition to supporting the board on regulatory compliance, they must pragmatically deliver on improving the organization's (cyber) resilience. Their role allows them to integrate the cyber, operational and reputational risk perspectives, which can participate in shaping executive strategy and long-term value creation.



**The primary mission of the CISO is to ensure that the organization delivers to its stakeholders the products and services that are core to the purpose of that business. To meet that mission, the CISO's primary job therefore is to protect the business. This is not easy. As this white paper points out, the digital infrastructure underpinning any given organization is, in reality, a series of embedded systems offering an often fuzzy view of knowable vulnerabilities exploitable by a dizzying array of threats. There is no finish line to security, rather it is an unrelenting exercise in risk management. And, although CISOs remain responsible for risk management, the rest of us remain responsible for security and must act accordingly.**

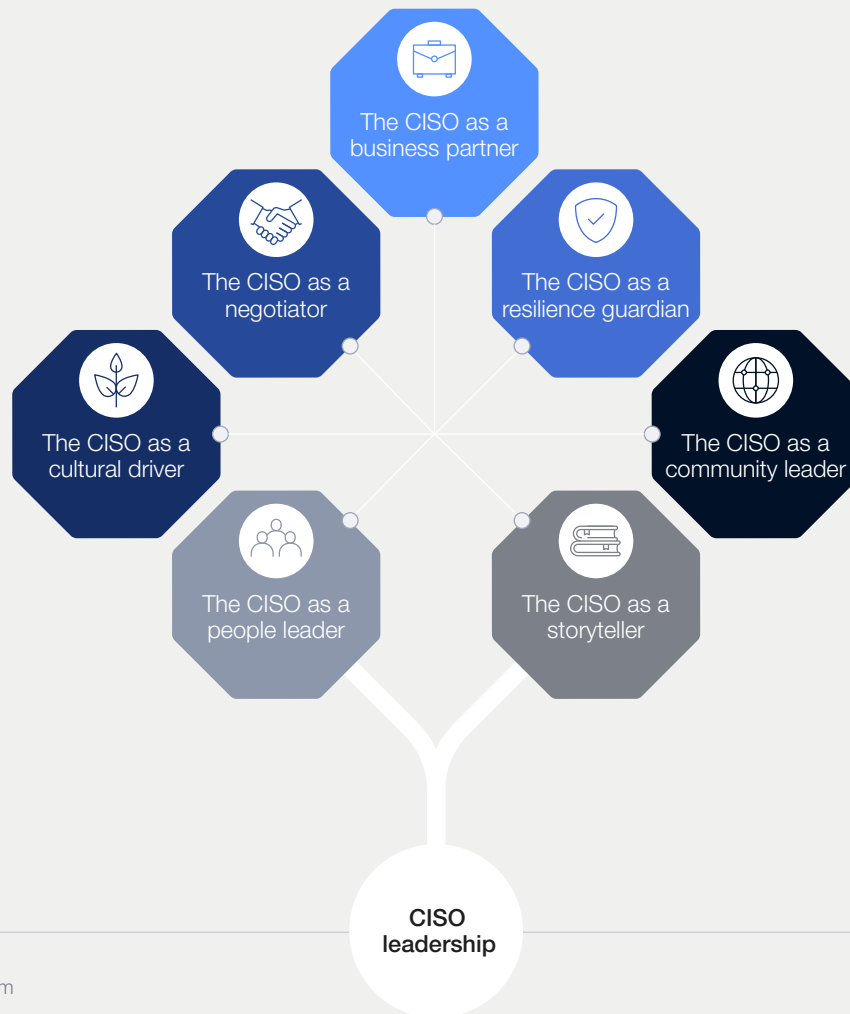
Kemba Walden, President, Paladin Global Institute

## 2.2 What can CISOs do to make the case for cybersecurity as a business imperative?

As the CISO role continues to expand in scope and influence, the definition of success is rapidly evolving. This section examines the critical enablers

that position CISOs to lead effectively within complex, dynamic and uncertain organizational and risk landscapes.

FIGURE 2 The building blocks of cyber leadership



Source: World Economic Forum

- 1. The CISO as a business partner:** Acting as a strategic business partner, the CISO balances risk and opportunity, enabling the safe adoption of new technologies and business models. Within this role, the CISO operates with a clear understanding of the organization's critical assets – the “crown jewels” – and ensures security efforts are directly tied to business priorities.
- 2. The CISO as a resilience guardian:** The CISO must be capable of standing firm in times of crisis, acting as a steady leader when the stakes are highest. CISOs must make clear decisions under pressure, guide response efforts and

maintain organizational confidence. In moments of uncertainty, the CISO becomes both a shield and a strategist.<sup>16</sup> CISOs need to be embedded in the wider enterprise resilience capability.

- 3. The CISO as a community leader:** CISOs should know their audience. This is essential so they can foster trust, build bridges and influence organizational culture at the industry level, the societal level and within their ecosystem, sometimes even serving as liaisons to external stakeholders such as regulators and governments. They must shape the organizational narrative taking into account their ecosystem's overall context.

4. **The CISO as a storyteller:** The CISO builds trust with internal and external stakeholders, such as the board or customers, by clearly communicating the organization's security posture and by translating technical safeguards into a compelling narrative that demonstrates transparency, accountability and a deep commitment to protection.
5. **The CISO as a people leader:** CISOs should provide their teams with structured training and certifications so team members can adapt to an evolving landscape while growing in their positions. The importance of soft skills, such as empathy and communication, should also be emphasized, and a leadership culture developed in which everyone has the potential to contribute to cybersecurity and take ownership of projects.
6. **The CISO as a cultural driver:** The CISO needs to establish a culture where everyone in the organization, from leadership to line employees, understands and participates in managing cyber risk. CISOs should not be the sole bearers of accountability.
7. **The CISO as a negotiator:** CISOs must operate as skilled negotiators, balancing security needs with business priorities and risk appetite. Whether advocating for resources, aligning with regulatory demands or influencing cross-functional decisions, effective negotiation is key to building trust and securing buy-in.

## 2.3 What can boards do to empower CISOs?






Boards can play a pivotal role in ensuring that their organization considers cybersecurity to be a business issue and elevates it as a strategic imperative. The World Economic Forum has led extensive collaboration within its various initiatives on the governance of cyber risk. Key publications include [Advancing Cyber Resilience: Principles and Tools for Boards](#) and [Principles for Board Governance of Cyber Risk](#). Those principles have also been tailored by some of the Forum's working

groups to different industries, such as the aviation, oil and gas and electricity industries.<sup>17,18,19</sup>

Within this, it is imperative that boards view CISOs as allies in this pursuit and therefore empower them to make an impact, as they are the ones who can create the success enablers for CISOs.

A number of enablers from boards can foster the CISO's impact:

FIGURE 3 Board enablers for CISO impact

 Establish a clear and independent CISO mandate	 Regularly and actively listen to the CISO	 Enable the CISO to develop relationships	 Ensure cyber risk management failures are fairly addressed	 Allocate a specific ring-fenced budget for cybersecurity
<ul style="list-style-type: none"> <li>— Is the CISO role empowered to provide an accurate and genuine view of the cyber risk posture of the organization without the fear of consequences?</li> </ul>	<ul style="list-style-type: none"> <li>— Is the CISO invited to board meetings, and is there allocated time to discuss cybersecurity topics?</li> <li>— Is the role visible and heard, and are findings acted upon by the leadership?</li> </ul>	<ul style="list-style-type: none"> <li>— Does the CISO have the mandate to develop strong relationships with their key stakeholders, including the board?</li> <li>— Is the collaborative nature of the role recognized, encouraged and enabled with internal and external stakeholders?</li> </ul>	<ul style="list-style-type: none"> <li>— Is there a mechanism in place to ensure that executives have a financial incentive to deliver on security outcomes?</li> </ul>	<ul style="list-style-type: none"> <li>— Is there a specific security and compliance budget allocated to the cybersecurity teams, including their tooling?</li> </ul>

Source: World Economic Forum

# Conclusion

The evolution of the CISO role provides an opportunity for top leadership to actively engage with cybersecurity issues and reframe cybersecurity as a strategic driver of value.

The accelerating complexity of the cybersecurity landscape is reshaping the responsibilities of organizational leaders. As digital ecosystems expand, supply chains intertwine and emerging technologies introduce new dimensions of risk, cybersecurity can no longer be treated as a siloed function. Instead, it must be recognized as a strategic concern that directly influences an organization's resilience, reputation and long-term growth. This reality implies that top leadership and boards must elevate cybersecurity from a technical concern to a boardroom priority, weaving it into the fabric of enterprise decision-making.

This shift is redefining the role of the CISO: the CISO mandate is expanding from securing systems to shaping enterprise resilience. Relationships are evolving: CISOs must be fluent in boardroom dialogue, able to engage internal and external stakeholders alike with clarity and influence. Tooling is becoming more integrated, making use of automation, AI and analytics to move from reactive defence to predictive capability. Culture, too, is critical: CISOs need to be architects of security-minded organizational behaviour, ensuring that every employee sees themselves as a steward of digital trust. Looking forward, the successful CISO

will not be measured only by their ability to prevent breaches, but by their capacity to embed security as a shared value across the enterprise.

An evolution such as this demands collective action. For CISOs, the call is to step up – to cultivate broader leadership skills, deepen their understanding of the business and expand their influence beyond the digital domain. For boards, the responsibility is to provide the mandate, resources and support structures that enable the CISO to succeed. This includes clarifying governance expectations, ensuring sufficient investment and creating direct lines of communication that elevate cybersecurity to a strategic concern. Together, these responsibilities form the conditions for success in a world where digital trust is inseparable from business continuity and growth.

Ultimately, the path forward requires close collaboration. As cyberthreats become more pervasive, organizations cannot rely on reactive measures or isolated expertise. In the coming years, the organizations that thrive will be those whose leaders treat cybersecurity not merely as defence, but as an enabler for trust, innovation and competitive advantage.



# Contributors

## Lead authors

### World Economic Forum

**Joanna Bouckaert**

Community Lead, Centre for Cybersecurity

**Isabella Kaplan**

Community Specialist, Centre for Cybersecurity

**Ellie Winslow**

Coordinator, Centre for Cybersecurity

## Acknowledgements

**Paige Adams**

Group Chief Information Security Officer, Zurich Insurance Group

**Ahmed Alketbi**

Chief Information Security Officer, Dubai Electricity and Water Authority

**Hessah A. Almajhad**

Chief Cybersecurity Officer, Saudi Information Technology Company (SITE)

**Mandy Andress**

Chief Information and Security Officer, Elastic

**Brad Arkin**

Chief Trust Officer, Salesforce

**Romain Aviolat**

Group Chief Information Security Officer, Kudelski Group

**Nik Bartholomew**

Vice-President, IT Cybersecurity & Risk Management, Occidental

**Erik Blomberg**

Chief Security Officer and Chief Information Security Officer, Handelsbanken

**Christophe Blassiau**

Senior Vice-President and Group Chief Information Security Officer, Schneider-Electric

**Grant Bourzikas**

Chief Security Officer, Cloudflare

**David Bradbury**

Chief Security Officer, Okta

**Stefan Braun**

Chief Information Security Officer, Henkel

**Scott Brown**

Chief Information Security Officer, Rio Tinto

**Ian Buffey**

Chief Information Security Officer, AtkinsRéalis

**Yanni Charalambous**

Vice-President and Chief Information Officer, Occidental Petroleum Corporation

**Nic Chavez**

Chief Information Security Officer, DataStax

**Sam Curry**

Global Vice-President and Chief Information Security Officer In Residence, Zscaler

**Martijn Dekker**

Chief Information Security Officer, ABN AMRO

**Deepen Desai**

Chief Security Officer, Zscaler

**Hazel Díez Castaño**

Chief Information Security Officer, Banco Santander

**James Dolph**

Chief Information Security Officer, Guidewire

**Alonzo Ellis**

Global Chief Information Security Officer, Morgan Stanley

**Yusuf Ezzy**

Chief Information Security Officer, PG&E

**Laurent Fabre**

Group Chief Information Security Officer,  
Pictet Group

**Sabrina Feng**

Chief Risk Officer, Technology, Cyber and  
Resilience, London Stock Exchange Group (LSEG)

**Frank Fischer**

Group Chief Information Security Officer, DHL  
Group

**Jacky Fox**

Senior Managing Director and Global Strategy  
Practice Lead, Accenture Security, Europe and  
Ireland, Accenture

**Janus Friis Bindslev**

Chief Digital Risk Officer, PensionDanmark

**Javier García Quintela**

Chief Information Security Officer, Repsol

**Daniel Gisler**

Chief Information Security Officer, Oerlikon

**Marco Arturo Guillen Gallegos**

Chief Information Security Officer, Coppel

**Dave Hannigan**

Chief Information Security Officer, Nubank

**Randy Herold**

Chief Information Security Officer, ManpowerGroup

**Yannick Herrebaut**

Chief Information Security Officer,  
Port of Antwerp-Bruges

**Lars Idland**

Vice-President, Security, and Chief Information  
Security Officer, Equinor

**Lawrence Jarvis**

Senior Vice-President and Global Chief Information  
Security Officer, Iron Mountain Information  
Management

**Stefan Jäschke**

Senior Vice-President and Head, Enterprise IT  
Security, Volvo Group

**Brad Jones**

Chief Information Security Officer, Snowflake

**Engin Kavaz**

Chief Technology Officer, Aydem Enerji

**Shaun Khalfan**

Senior Vice-President and Chief Information  
Security Officer, PayPal

**Iftekhar Khan**

Chief Information Security Officer, JS Bank

**Matthew Knight**

Chief Information Security Officer and Head of  
Security, OpenAI

**Thomas Koch**

Chief Security Officer, SIX Group

**Sigmund Kristiansen**

Chief Cyber Security Officer, Aker BP

**Michael Lashlee**

Executive Vice-President and Chief Security Officer,  
Mastercard

**Frederik Lilleøre Jæger**

Chief Information Security Officer, Orsted

**Koos Lodewijkx**

Chief Information Security Officer, IBM

**Chris Lyth**

Chief Information Security Officer, Arup Group

**David Mabry**

Vice-President and Chief Information Security  
Officer, Gulfstream Aerospace

**David Mamikonyan**

Chief Security Officer, MGX

**Derek Manky**

Chief Security Strategist and Global Vice-President,  
Threat Intelligence, Fortinet

**Raffaele Maresca**

Chief Information Security Officer, Technip Energies

**Kevin McCarty**

Chief Information Security Officer, Gartner

**Lance McGrath**

Chief Security Officer, Danske Bank

**Rishi Mehta**

Group Chief Information Security Officer, HCLTech

**Michael Mestrovich**

Chief Information Security Officer, Rubrik

**Ben Miller**

Chief Information Security Officer, Dragos

**Eiichiro Mitani**

Executive Partner, Mitsubishi Electric

**Deryck Mitchelson**

Global Chief Information Security Officer, Check  
Point Software Technologies

**Paulo Moniz**

Head, CyberSecurity and Information Technology  
Risk, EDP – Energias de Portugal

**Luís Filipe Morais**

Chief Information Security Officer, Galp

**Claus Norup**

Group Chief Information Security Officer, Euroclear

**Yonesy Núñez**

Chief Cybersecurity Risk Officer, Depository Trust and Clearing (DTCC)

**Barbara O'Neill**

Global Chief Information Security Officer, EY

**Natalia Oropeza**

Global Chief Cybersecurity Officer and Chief Diversity and Inclusion Officer, Siemens

**John Petersen**

Chief Information Security Officer, Nestlé

**Christoph Peylo**

Chief Cyber Security Officer, Robert Bosch

**Cezary Piekarski**

Group Chief Information Security Officer, Standard Chartered Bank

**Manoj Puri**

Chief Security Officer, Absa Group

**Yuri G. Rasega**

Head of Cybersecurity, Enel

**Ramesh Razdan**

Global Chief Technology Officer, Bain & Company

**Cyril Reol**

Group Chief Information Officer, Mercuria Energy Group

**Miguel Angel Rodríguez Alvarez Icaza**

Chief Technology Officer, Kapital

**Jason Ruger**

Chief Information Security Officer, Lenovo

**Mehzad Sahar**

Group Chief Information Security Officer, Engro

**Alexander Schellong**

Managing Director, Cybersecurity, Schwarz Digits, Schwarz Group

**Ralf Schneider**

Allianz Senior Fellow; Head, Cybersecurity and NextGenIT Think Tank, Allianz

**Sachit Singh**

Senior Director, Cyber Security, OakNorth

**Kristoffer Sjöström**

Chief Security Officer and Head, Group Security and Cyber Defence, Skandinaviska Enskilda Banken (SEB)

**Shiv Srivastava**

Chief of Information Technology, Indorama Ventures

**Mark Swift**

Chief Information Security Officer, Trafigura Group

**Satoshi Takeda**

Director, Senior Vice-President, Chief Development Officer and Chief Information Officer, Mitsubishi Electric

**Alex Tiley**

Chief Information Security Officer, CLS Bank International

**Akhilesh Tuteja**

Global Cyber Security Leader, KPMG

**Cyrus Vance**

Partner, Baker McKenzie

**Prashant Verma**

Head, Information Security (Chief Information Security Officer), Bajaj Finance

**Kemba Walden**

President, Paladin Global Institute, Paladin Capital Group

**Maynard Webb**

Founder, Webb Investment Network

**Tom Wilson**

Senior Vice-President and Chief Information Security Officer, Southern Company

**Carl Windsor**

Chief Information Security Officer, Fortinet

**Jelena Zelenovic Matone**

Chief Information Security Officer, European Investment Bank

**Adam Zoller**

Chief Information Security Officer, CrowdStrike

## World Economic Forum

### **Chiara Barbeschi**

Specialist, Cyber Resilience,  
Centre for Cybersecurity

### **Filipe Beato**

Lead, Centre for Cybersecurity

### **Sean Doyle**

Lead, Cybercrime Atlas Initiative, Centre for  
Cybersecurity

### **Tal Goldstein**

Head of Strategy, Centre for Cybersecurity

### **Giulia Moschetta**

Initiatives Lead, Centre for Cybersecurity

### **Natasa Perucica**

Project Lead, Centre for Cybersecurity

### **Luna Rohland**

Specialist, Cyber Resilience,  
Centre for Cybersecurity

### **Apisada Suwansukroj**

Lead, Programming and Communications,  
Centre for Cybersecurity

### **Kesang Tashi Ukyab**

Lead, Cyber Resilience, Electricity,  
Centre for Cybersecurity

### **Natalia Umansky**

Project Specialist, Cybercrime Atlas Initiative,  
Centre for Cybersecurity

---

## Production

### **Bianca Gay-Fulconis**

Designer, 1-Pact Edition

### **Tanya Korniichuk**

Illustrator, 1-Pact Edition

### **Simon Smith**

Editor, Astra Content



# Endnotes

1. European Parliament and Council of the European Union. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)*. Official Journal of the European Union, L333, 80–152. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555>
2. World Economic Forum. (2025, January 13). *Global cybersecurity outlook 2025*. <https://www.weforum.org/publications/global-cybersecurity-outlook-2025/>
3. Microsoft Corporation. (2024). *Microsoft digital defense report 2024*. <https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024>
4. World Economic Forum. (2025, January 21). *Artificial intelligence and cybersecurity: Balancing risks and rewards*. <https://www.weforum.org/publications/industries-in-the-intelligent-age-white-paper-series/cybersecurity/>
5. World Economic Forum. (2025, January). *AI in action: Beyond experimentation to transform industry*. [https://reports.weforum.org/docs/WEF\\_AI\\_in\\_Action\\_Beyond\\_Experimentation\\_to\\_Transform\\_Industry\\_2025.pdf](https://reports.weforum.org/docs/WEF_AI_in_Action_Beyond_Experimentation_to_Transform_Industry_2025.pdf)
6. World Economic Forum. (2025, April 24). *The cyber resilience compass: Journeys towards resilience*. <https://www.weforum.org/publications/the-cyber-resilience-compass-journeys-towards-resilience/>
7. Inside Google. (2025, March 18). *Google announces agreement to acquire Wiz*. <https://blog.google/inside-google/company-announcements/google-agreement-acquire-wiz/>
8. Global Cybersecurity Forum and Boston Consulting Group. (2024). *2024 cybersecurity workforce report: Bridging the workforce shortage and skills gap*. <https://web-assets.bcg.com/61/d3/705fbd684d70b0e5f98cdf7cf47/2024-cybersecurity-workforce-report.pdf>; ISC2. (2024, September 11). *Growth of cybersecurity workforce slows in 2024 as economic uncertainty persists*. <https://www.isc2.org/Insights/2024/09/ISC2-Publishes-2024-Cybersecurity-Workforce-Study-First-Look>
9. World Economic Forum. (2024, April 28). *Strategic cybersecurity talent framework*. <https://www.weforum.org/publications/strategic-cybersecurity-talent-framework/>
10. Fortinet. (2024). *2024 cybersecurity skills gap*. <https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf>
11. ISACA. (2024, October 1). *State of cybersecurity 2024*. <https://www.isaca.org/resources/reports/state-of-cybersecurity-2024>
12. Standard Chartered. (2018, October 18). *Fighting financial crime with cybersecurity insights*. <https://www.sc.com/en/news/fighting-financial-crime-with-cybersecurity-insights-2>
13. World Economic Forum. (2021, March 23). *Principles for board governance of cyber risk*. <https://www.weforum.org/publications/principles-for-board-governance-of-cyber-risk/>
14. Tooling is the suite of technical solutions, platforms and technologies used to support an organization's cybersecurity strategy and operations, which the CISO oversees, integrates and optimizes to detect, prevent and respond to cyber threats.
15. Accenture. (2023, June 12). *State of cybersecurity resilience 2023*. <https://www.accenture.com/us-en/insights/security/state-cybersecurity>
16. World Economic Forum. (2025, April 24). *The cyber resilience compass: Journeys towards resilience*. <https://www.weforum.org/publications/the-cyber-resilience-compass-journeys-towards-resilience/>
17. World Economic Forum. (2019, February 13). *Cyber resilience in the electricity ecosystem: Principles and guidance for boards*. <https://www.weforum.org/publications/cyber-resilience-in-the-electricity-ecosystem-principles-and-guidance-for-boards/>
18. World Economic Forum. (2021, April 14). *Pathways towards a cyber resilient aviation industry*. <https://www.weforum.org/publications/pathways-towards-a-cyber-resilient-aviation-industry/>
19. World Economic Forum. (2021, May 17). *Cyber resilience in the oil and gas industry: Playbook for boards and corporate officers*. <https://www.weforum.org/publications/cyber-resilience-in-the-oil-and-gas-industry-playbook-for-boards-and-corporate-officers/>



---

COMMITTED TO  
IMPROVING THE STATE  
OF THE WORLD

---

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

---

World Economic Forum  
91–93 route de la Capite  
CH-1223 Cologny/Geneva  
Switzerland

Tel.: +41 (0) 22 869 1212  
Fax: +41 (0) 22 786 2744  
[contact@weforum.org](mailto:contact@weforum.org)  
[www.weforum.org](http://www.weforum.org)