Teneo | TAG CYBER

Teneo Cyber Insights Series for CEOs

2023 is the Year to Formalize the CISO to CEO Reporting Structure

Teneo Insights / May 2023

In our first "Teneo Cyber Insights Series for CEOs" article, we highlighted how recent innovations in AI have amplified the profound changes and complexity in the cybersecurity realm. The second entry in the series discussed the need for global organizations to ensure that cybersecurity contemplates geopolitics as an integral part of the corporate risk equation, particularly as it relates to critical infrastructure.

When you factor in the evolving and increasingly sophisticated threat landscape, and what promises to be a concerted future regulatory and compliance response to address these challenges, the job of the Chief Information Security Officer (CISO) has only become more intense and more important. And why? Because the CEO is also worried about these issues and is being asked at every turn by stakeholders to ensure these issues are on her/his agenda. As such, we believe it is time to solidify a reporting structure whereby the CISO reports directly to the CEO as the norm for corporations.

We have seen a lot of churn in the CISO profession, hallmarked by burnout and a lack of voice, visibility and funding from the executive suite. Layer on the inevitable cyber-attack, and the CISO is often the one forced to exit in the aftermath. This can create a revolving door of tools and technology and lead to instability in an organization's technical operations, technical debt and increased vulnerability.

Much analysis has been done as to the various reporting constructs for the CISO, whether reporting to a CIO, a CFO/Chief Risk Officer or the CEO. Such analysis highlights the pros of greater visibility with the CEO, strategic alignment with the CIO or direct access to budget when the CFO has direct oversight. Cons include the inability for the CEO to focus on cyber as much as the CISO would need, competing priorities between the CIO and CISO function and a CFO perhaps not understanding or prioritizing cybersecurity. Other cybersecurity experts and organizational consultants suggest that the reporting decision may be industry-specific or business dependent, which is understandable. However, we submit once again that the emerging and irrevocable societal and business changes introduced by artificial intelligence, geopolitical trends and cyber complexities touching all organizations today transcends a sectoral approach and paves a path for ubiquity in the CISO to CEO reporting line.

To further articulate the opportunity, it is important to explain this perspective from two angles. In 2023 and beyond, in light of the aforementioned developments in cybersecurity, what does it mean to and for the CEO if they have the CISO as a direct report vs not?

Stakeholders are expecting the CEO and the organization they oversee to have a risk management strategy that addresses cybersecurity risks as well as an appropriate and strategic response should risks become a reality.

The CEO already has a big job, further exacerbated by increasing risk in the digital sphere as more business processes go online, get support from artificial intelligence or come under more sophisticated cyber-attack. Boards and other key constituents such as shareholders, investors, the media, regulators and employees have a lot of questions today for the CEO about how those risks are being tracked, managed and mitigated. That responsibility sits with CISOs. While much of the detail regarding how those risks manifest and the associated mitigation tools and processes can be quite technical in nature, the CEO needs greater fluency in some of these details framed in a business context to counter these risks. Stakeholders are expecting the CEO and the organization they oversee to have a risk management strategy that addresses cybersecurity risks as well as an appropriate and strategic response should risks become a reality.

What does the CISO to CEO direct reporting structure enable?

That direct partnership and chain of command from CISO to CEO gives the lead executive direct visibility to their cybersecurity risk management strategy and forces the CISO to frame cybersecurity in a business context so that a non-technical CEO can understand. The direct reporting relationship can also provide the CISO with the type of access to the longer term growth and innovation strategies envisioned by the CEO, which enables the CISO to plan first-hand and have a security design role early on in the process.

The proximity to the CEO means that a CISO may also have a greater shot at budget prioritization for cybersecurity. Furthermore, a CEO who is increasingly fluent in the cybersecurity strategy for the organization and prioritizes cybersecurity spend, security controls and security strategy, is more likely to drive a top-down culture of security awareness and security mindedness across the organization. There are a series of potential drawbacks related to this proposed reporting structure, namely competing objectives, tension between the

CISO and CIO and the potential inability for the CISO to capture the attention of the CEO (for reasons attributed to lack of CEO focus on day-to-day operational issues). However, we argue that the changing risk landscape necessitates a CISO to CEO direct relationship, enabling collaboration on emerging matters related to cybersecurity, AI adoption and implementation risk whether from a technology, security, ethics and/or compliance perspective. CISO engagement alongside the CEO on these issues is vital to ensure the benefits of innovation and growth are balanced with appropriate security considerations and mitigations. In the process, the closer relationship will elevate the role of the CISO and her/his initiatives to the board and across the C-suite. Lastly, this relationship will prove invaluable in the throes of a significant cyber event where the executive team, and in particular the CEO, needs a reliable, proven and trust-based source of information and incident response partner.

How may the CEO be disadvantaged without this reporting structure?

While some may feel that the CEO benefits from one less direct report, it is our belief that CEOs benefit more from having an internal advisor who is steeped in all matters information technology or operations technology security (depending on the business) and can proactively help the CEO parse through the important stuff to withstand stakeholder questioning and scrutiny. In the absence of such an important advisor and immediate direct report, potential hierarchical reporting structures could either dilute, misrepresent or delay important information from reaching the CEO in a timely fashion.

The CISO role has been working hard for at least a decade to change the narrative about the role from blocker to business growth enabler. As such, the information security profession and the individuals aspiring to a C-suite role as CISO have been focusing more and more of their personal business development toward demonstrating how information security can help organizations more safely and securely innovate as the threat landscape changes. If the CEO isn't able to champion growth and innovation through the lens of "security by design" advisory and recommendations through frank talk with their CISO, the organization may unnecessarily evolve to become more vulnerable and less resilient.

What does the 2023 CISO look like?

If CEOs subscribe to these ideas, the next step is to ensure that the CISO embodies the necessary capabilities and qualities to support the CEO. The CISO must have a clear understanding of the business context in which the organization operates, including the organization's mission, vision, strategic objectives, stakeholder universe (and their expectations) and their regulatory and compliance requirements. In practice, this means that the CISO must not only have technical aptitude – she/he must also be a strategic thinker who can clearly communicate concepts to non-technical stakeholders. Once empowered by the CEO – and that empowerment is key – a CISO must be able to engage with the organization's leadership team and board to ensure that cybersecurity is given the necessary attention and resources. As a trusted advisor and direct report on the matter of cybersecurity risk management, the CISO will need to have the constitution to push back on or challenge the CEO if the mission strays in ways that makes the organization more vulnerable without considering and implementing relevant mitigations. As such, the CISO must be grounded in threat intelligence and able to work with the CEO, C-suite and the board to balance risk tolerance and innovation.

This evolution in the information security profession and the CISO job function will help elevate the CISO to a senior-level, direct report to the CEO, which will then turn the CISO into a more desired executive role and ultimately make organizations more resilient.

Authors

Ed Amoroso
Senior Advisor, Teneo
CEO TAG Infosphere, Inc., Research Professor, NYU and Senior Advisor to Teneo Risk

Courtney Adante
President, Teneo Risk Advisory
Teneo Cybersecurity Client Lead and Cyber Crisis Management Advisor

Sophie De Ferranti
Senior Managing Director
Teneo People Advisory, Global Cybersecurity Practice Lead

Teneo®
The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions, and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance, ESG and DE&I.

The firm has more than 1,600 employees located in 40+ offices around the world.

teneo.com

About TAG Cyber

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 500 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth guidance, market analysis, consulting, and personalized content based on thousands of engagements with clients and non-clients alike—all from a practitioner perspective.

www.tag-cyber.com.