CISO Cross-Industry

Expert Exchange

Q1 Executive summary
January 30, 2024

kyndryl

Overview

In this Expert Exchange session, fifteen CISOs convened to discuss the evolving role of CISOs in cybersecurity and risk management. The agenda was based upon mutual interests of participating CISOs collected in advance during one-on-one interviews.

Host

Michael Restivo
Kyndryl, USA Vice President – Security and Resiliency

SME

Kris Lovejoy
Kyndryl, Global Practice Leader – Security and Resiliency

Key topics

PAGE
03 Security and Resilience Leadership

04 The Evolving Role of CISO in Cybersecurity Governance and Risk Management

05 Defense Strategies, Disaster Recovery, and Regulations

06 CISO Reporting and Risk Management Roles

Security and Resilience Leadership

- CISOs are witnessing a heightened focus on cybersecurity from their boards. Board members are paying more attention to issues such as criminal penalties, criminal liability for failure to comply with regulatory acts, rising insurance premiums, and credit risk. As a result, there has been a shift in the operational responsibilities of CISOs, particularly those subjected to the Digital Operational Resilience Act (DORA) and FCC.

- As boards are educated on the new requirements for cybersecurity, there are several obligations that they must focus on. These include governance and management structures in terms of whether their organizations have implemented the required cyber management frameworks, who is responsible for those frameworks, whether there is the right infrastructure in place, material incident identification practices, and whether management teams can identify and escalate these issues.

> "The question of enhanced governance is really driving boards to ask questions as to whether or not the management structure that has been established to manage risk is effective enough for them to feel comfortable and confident that the organization is performing the activities they need to perform."
>
> — Kris Lovejoy,
> Global Practice Leader –
> Security and Resiliency, Kyndryl

The Evolving Role of CISO in Cybersecurity Governance and Risk Management

- Many boards are rethinking the scope of responsibility for the CISO as organizations become more digitally centric and risk extends beyond cybersecurity. Operational resilience is a key focus given the world of commerce is highly dependent on digital infrastructures. These infrastructures can be impacted by software outages, network outages, environmental-related outages, and cybersecurity-related outages.

- In some cases, the CISO function is being expanded to include business continuity and disaster recovery, and potentially some other capabilities within that context. Many organizations are forging closer synergies between resilience and recovery by either placing the CISO on teams with IT leadership or having them work closely with disaster recovery teams.

- The roles of the CISO and Chief Resiliency Officer (CRO) are intertwined, making it difficult for organizations to separate them. However, there are fundamental differences between the two roles in terms of remit and focus. CISOs work with the different business owners to build business continuity plans and business impact analyses but do not own those plans because they do not own those businesses. CROs, on the other hand, must know how a business is going to survive in the face of a challenge and own the business continuity plans which they must execute regardless of whether IT is engaged or not.

> “We need to combine these things. It’s not just security risks—we’re just talking about technology risks and use the exact same words. Security is just one of the risks. So, as we start driving this from the top down, we need to have a view that is risk-based.”
>
> — CISO Expert Exchange Member

What IT decision makers say about the state of IT risk

Learn more →

Defense Strategies, Disaster Recovery, and Regulations

- CISOs are working to clarify the three lines-of-defense model for risk management processes. Due to the various patterns in the risk management process, auditors are demanding a crisp definition of the three lines of defense. There is some debate around whether the CISO belongs in IT as a line-one function, or whether IT belongs in the second line of defense.

- One view on the model is that the line owning that particular step in the process should be used to identify who goes where, whether CISO or CRO or any other title assigned to such an individual. For instance, while it is the business that should typically do the first line of risk identification, the CISO or resiliency officer should do the second line which includes prioritizing the risk and managing the implementation of the policy. However, there are gray areas when it comes to testing and monitoring of controls, as well as investigation and response because of the overlaps between line-one and line-two functions.

- Emerging regulations, especially within the NIST framework, are based on an architecture and mode of practice that is 10 years old, making them difficult to comply with in today's hybrid work environment. For instance, when working remotely, one is under ISP, and the zero trust model comes into effect. Unless the regulations consider the hybrid work environment, businesses may become non-compliant.

> "There's a lot of overlap between line-one and line-two functions, and that is causing a lot of confusion as well, particularly on testing controls."
>
> — Kris Lovejoy,
> Global Practice Leader –
> Security and Resiliency, Kyndryl

Kyndryl Security Assurance Services

Learn more →

CISO Reporting and Risk Management Roles

- Organizations differ in where they have the CISO report. In one example, the CISO reports to the CIO and CTO, leading to a strong collaborative working relationship across all the technology towers, particularly driven by the tone from the top. In another example, the CISO reports to the Chief Digital Officer. A common complaint from CISOs that are reporting into the first line, typically IT organizations, is that they are being pressured to give up territory.

- When reporting to boards, the CISO should report all risks that the business faces since security is not an operational or resiliency problem but rather a risk problem. Boards are increasingly thinking of operational resilience as being more than technology, thus pushing the CISO outside the realm of technology and elevating them to a kind of risk process owner, responsible for understanding the overall integrity, availability, and confidentiality of data as well as the availability and integrity of the systems that provide that data and deliver those services.

> "My customers want to see that we have considered security upfront, that we are compliant with high trust. If I am embedded in only the technology space and resiliency of our operational servers, I have lost focus of the rest of the business and I have removed myself from where I think I actually have a much bigger impact on my ability to secure and prevent risk."
>
> — CISO Expert Exchange Member

The CISO Thought Leadership Expert Exchange is hosted by Kyndryl, Inc. Please contact Mike Restivo or Kris Lovejoy for any questions about Kyndryl or this Exchange.

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.

03-10-2023