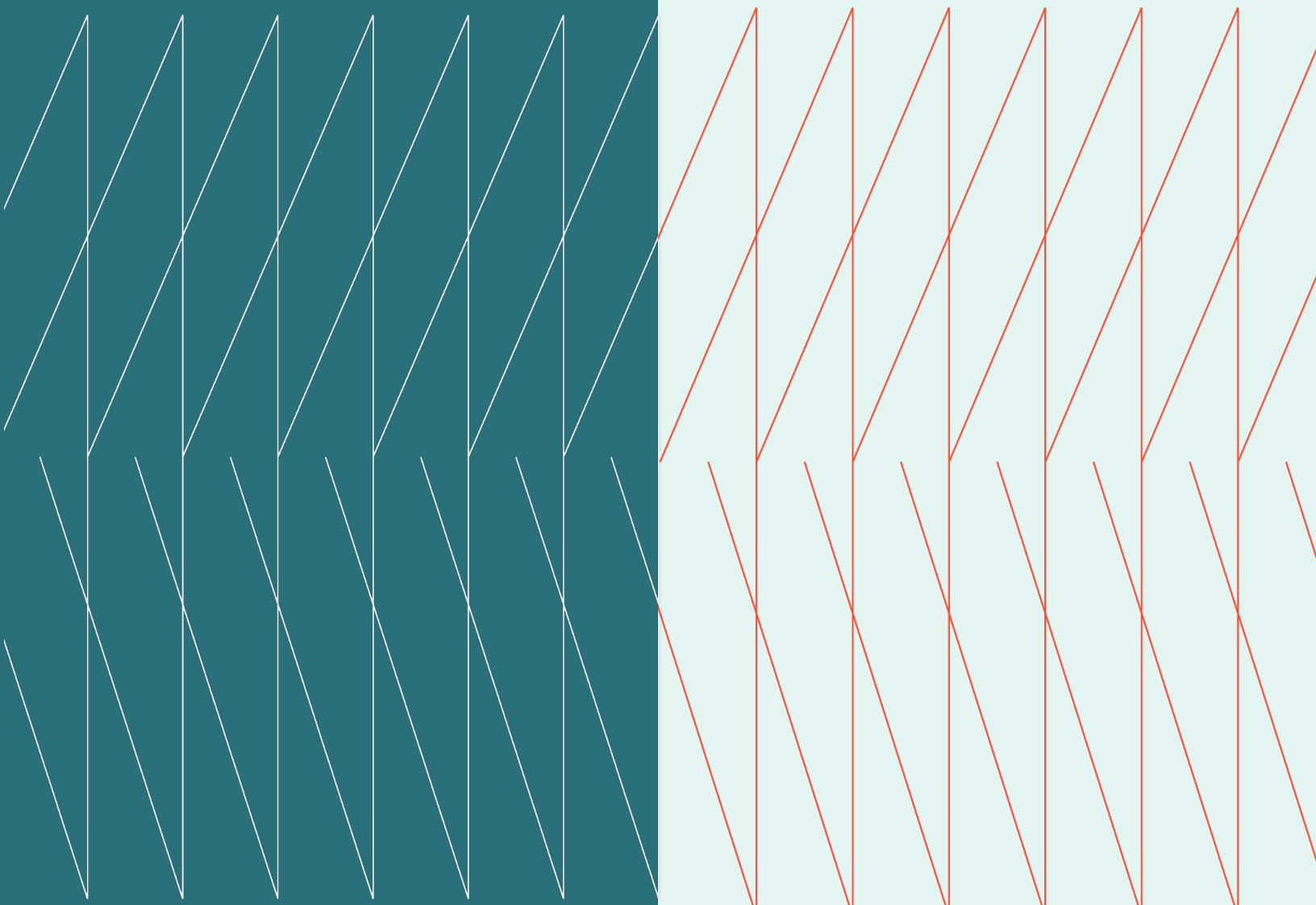
CISO

Expert Exchange

February 27, 2025

kyndryl

Executive Summary



Hosts:

Denis Villeneuve
Cybersecurity and Resilience Practice Leader, Kyndryl Canada

Kris Lovejoy
Global Security and Resiliency Practice Leader

Overview

In this Exchange session, several CISOs convened to discuss cybersecurity regulations, compliance, and board engagement.The agenda was created based on advance interviews with participants.

Expert Exchange themes

- The Evolving Regulatory Landscape
- Complying with Regulations
- Communicating with the Board around Cybersecurity

The Evolving Regulatory Landscape

- Globally, a significant number of new regulations are being introduced with the aim of creating more secure and resilient digital environment that protect critical infrastructures and maintain public trust in digital services. This surge of regulation comes in parallel to various challenging factors for CISOs: a dramatic increase in the attack surface since COVID; a great number of technologies approaching end of life; and companies migrating to the cloud rapidly but neglecting to refactor their applications – instead opting for containerization of legacy apps. All these factors have pushed CISOs to move toward establishing a better baseline of security controls.

- Many of the new regulations are primarily focused on the “meat and potatoes" basics of security controls. Some also touch on the recovery and resiliency side, since even organizations with adequate protections often lack the ability to recover in the event of an attack. A third area of focus is on the supply chain, as the supply chain—particularly smaller suppliers—became targets of attacks during COVID.

- Even as most countries pursue greater cyber regulation, they are not doing so in lockstep. Kyndryl foresees a balkanization of regulations as countries develop very country-specific rules, which will result in much greater compliance complexity for companies operating globally. DORA and NIST are good "barometers" of what could be coming with respect to basic cybersecurity controls.

- Regulations in Canada are in flux as well. After years of work, Bill C-26 is expected to die on the floor amidst the change in government. However, Bill 194 in Ontario has similar elements and could be a step towards establishing necessary regulations to protect the government and protect critical infrastructure. Companies should ensure that any programs they're putting in place align with the frameworks of these bills.

- “There are 150 countries on earth, and of those, 90 have introduced cybersecurity regs or resiliency regs over the past two years designed to enable critical infrastructure industries to improve their overall security resiliency capabilities.” – Kyndryl Canada CISO Exchange Member.

Complying with Regulations

- Rather than viewing compliance as a burden, many CISOs see it as a positive. Compliance with security standards elevates security throughout an organization and, with it, the voice of the CISO. It also enables CISOs to focus on areas such as supply chain and application security. Furthermore, if an organization is pursuing security in the right way, regulations typically complement rather than disrupt what the company is already doing.

- A member noted that it's crucial to establish data sovereignty and residency upfront because it is hard to backtrack once data is already being shared across industries and borders. It's challenging (but necessary) to establish among institutions that share heavily (for example, universities) and when using hyperscalers with global footprints.

- One CISO shared the view that companies get serious about security for business reasons, not compliance reasons, and relying on regulation to direct their security program puts a company behind. Companies need to get ahead of threats instead of waiting for regulations to catch up. If a company is leading on security, regulations are useful in reinforcing approaches and convincing senior leaders that the organization is on the right track.

- Since most regulators go through a process of consultation before proposing anything, it is important for business leaders to engage in the process and provide feedback. The more companies build relationships with regulators, the more influence they can have on regulations.

- "It's important to do things for the right reason, not necessarily just for the purpose of getting a check mark somewhere in some document. The more you can explain that you're doing something not because a regulator asked for it but because it's the right thing to do, the more stable it is in the long run. Otherwise, it comes across as a knee-jerk reaction, and then you're always behind the eight ball because you're never like forward thinking; you're just waiting for somebody to tell you what to do." – Kyndryl Canada CISO Exchange Member.

Communicating with the Board around Cybersecurity

- Due to differences in backgrounds and areas of focus, CISOs often need to adjust their approaches when engaging their boards. Board members are primarily concerned with financial risk and risks to shareholders. This perspective, combined with the fact that most are not technologists, can make it difficult for board members to understand cybersecurity as it is often presented. The key is to frame cybersecurity in the context of how they relate financial risks, which boards will better understand.

- When presenting to boards around cybersecurity, it is essential that CISOs align metrics to risk tolerances. CISOs can help boards define risk appetites around cybersecurity by connecting disruptions to financials (for example, an outage of one to two hours equates to x amount of revenue loss, etc.) Once risk tolerance is established, CISOs can develop metrics to measure how their program is fairing and demonstrate where investment is needed.

- A similar approach is to connect cybersecurity to the company's goals, both the overall goals and the different goals for areas of the business. In this case, the conversation is on the same topic and the same information, but from a different view. For example, talking to management about technology and investments is one type of conversation, while talking with the board is another.

- In some organizations, senior leaders have the mindset that they are secure since no cyber-attacks have ever happened to them. In such cases, CISOs can rely on compliance to support their positions and convince leaders that changes must be made. This is not as effective as having buy-in from board members, but it is at least a start since regulation can't be ignored.

- Especially when there is no cyber expert on the board, it is critical that CISOs educate members on cyber risks. Asking them to define tolerances without understanding risks can lead to unrealistic expectations, so CISOs must help them understand what cyber risk really means. This is especially true when boards assume that spending more money will make everything fine when, in fact, attacks are still possible even with more investment.

- "It's hard for a board member to think about cyber because A, most of them are not technologists and B, they tend to think about it from a financial context. So, one of the things you have to begin to do is force them to think about risk in a different way." – Kyndryl Canada CISO Exchange Member

To learn more about the Kyndryl Canada CISO Expert Exchange or to become a member of this community, please contact Matthew Johnson.

kyndryl