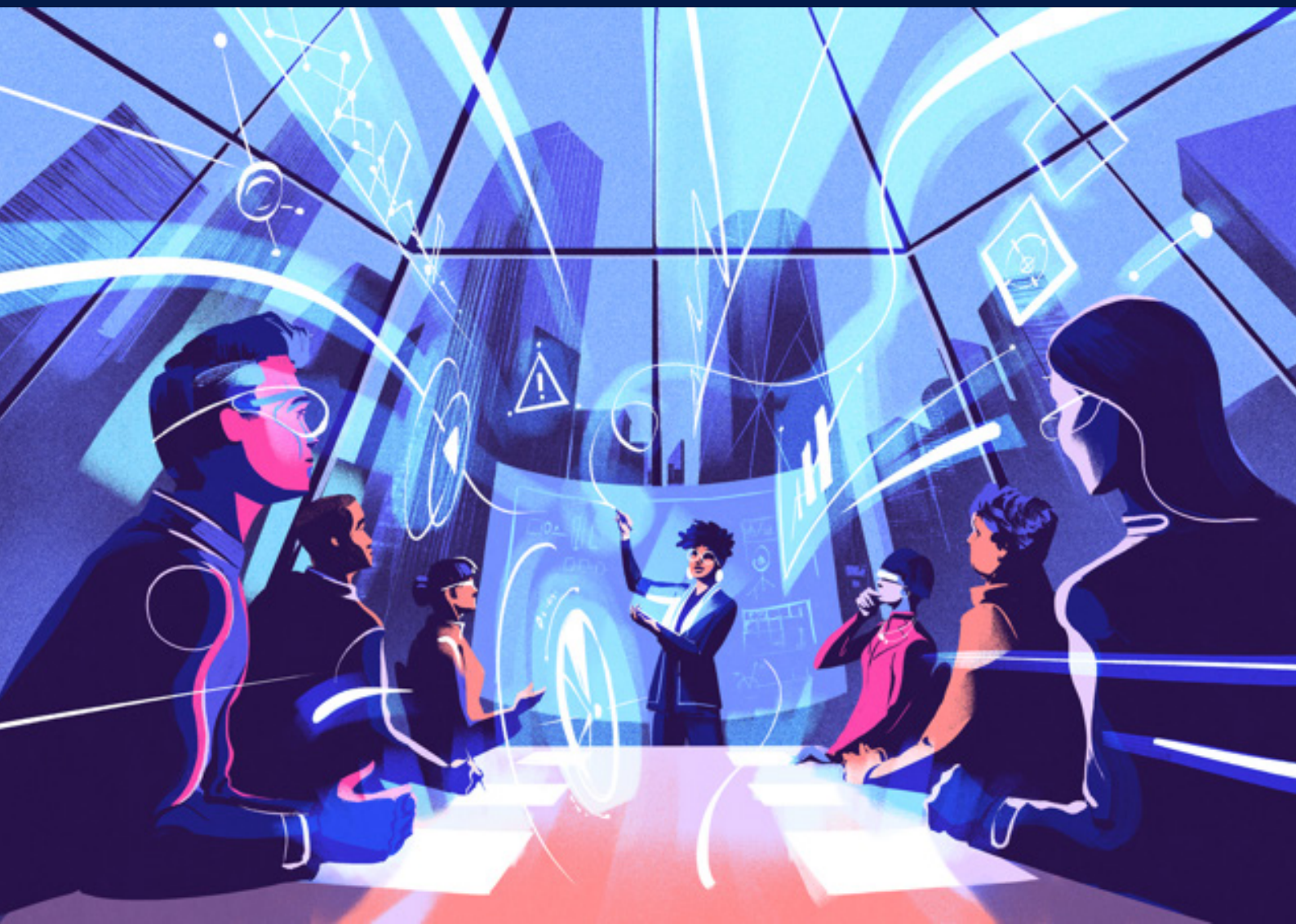
ISTARI Perspectives

Mistakes and Lessons from Interacting with the Board on Cybersecurity

Jason Mallinder

06 • 2024



Mistakes and Lessons from Interacting with the Board on Cybersecurity

I distinctly recall walking into the boardroom in the early days of my tenure as a CISO at a prominent global bank. I wanted to highlight a serious cyber risk to the board: the potential loss of data via active USB ports. I was proposing to lock them down.

But the board meeting did not go as I had intended. I was perceived as restricting business. One comment I received was that the data was highly complex and extremely difficult to make meaningful by the bank itself, so how would any outsider do much harm with it? It ended up being a very challenging meeting.

I returned two months later, this time equipped with better data and a different approach. For example, I showed how many gigabytes of data were put on USB drives each month. This time, the board's response was a resounding acknowledgement: "You need to restrict USB ports."

For many executives, even the most senior ones, a presentation to the board of directors is the most demanding test of leadership communications. CISOs also commonly struggle. While conventional advice like "tell a story" or "use fewer bullet points" holds true, it often falls short in addressing the unique challenges certain scenarios present.

I have had many personal experiences engaging with boards during my tenure as a CISO and have discussed the topic with many peers over the past few years. Below are the lessons and insights I've gathered in the hope of helping others should they have to present to their board.

Why reporting to the board is different – and difficult

The boardroom is a distinct forum that requires a specific type of presentation and preparation. In most cases, the slides will have been vetted by one or two board members before the meeting and the directors likely will have examined the material beforehand. Too often, presentation slots to the board are limited to 10-15 minutes but rushing through the slides fails to deepen the board's understanding of the key topic or showcase the executive's leadership skills.

Another challenge is that the board of directors is a unique and heterogeneous forum with no comparison to other groups most executives regularly engage in. It often comprises business leaders, academics, former CEOs and current financial officers, bringing expertise from different industries and fields. Some members have served on boards for decades; others may be brand new.

When reporting to the board, the objective is not to discuss quarterly KPIs or other information that's readily available — board members can access that on their own. Instead, the presentation should cover the most pressing challenges the organisation is facing (in plain language) and outline how to address them. Remember, the board has to be able to evaluate all enterprise risks.

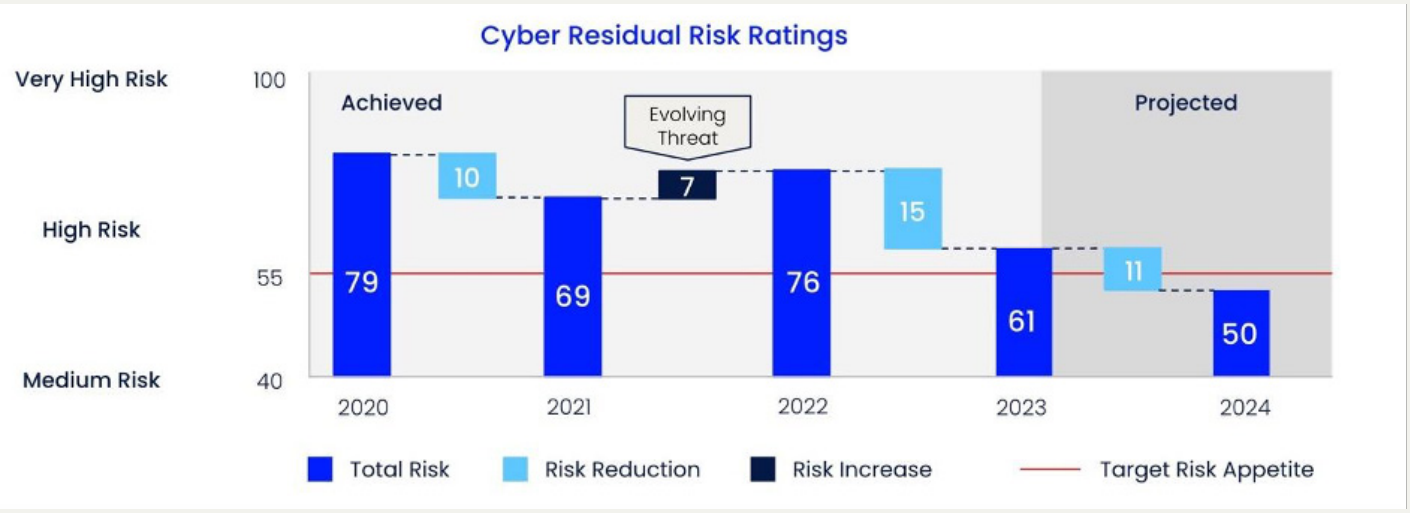
What I would report

Having tried different approaches over the years, I found the following structure most useful: focus on changes in the threat landscape, progress in controls and reduction of business risk alongside any investments required.

Risk & investment: This was often the most important part of my presentation, so I would start and finish with it. In this section, I summarised the level of risk reduction achieved over time in line with the organisation's risk appetite and enterprise risk, using a scale and indicative dollar values to try to avoid a financial conversation. I demonstrated the effectiveness of our risk mitigation strategies and their alignment with the business's risk appetite. I then would outline any necessary upcoming investments in controls for sustained risk reduction, including budget considerations for cybersecurity initiatives and their expected impact on the overall risk posture.

Threat landscape: The threat landscape is vast and many threats might not apply to the organisation. When presenting the changes in the internal and external threat landscape, I always highlighted why those changes mattered to the organisation. My report included a comprehensive analysis of current threats, encompassing both internal and external factors. I also included a section on emerging threats that potentially could impact the organisation in the medium and long term.

Controls: Following the threat landscape, I focused my update on any progress in implementing controls, emphasising what that meant in a business context. They naturally focussed more on technical controls, because they are easier to measure than people and culture. I would explain the significance of these controls in combatting threats and illustrate how they contributed to safeguarding critical assets, ensuring compliance and maintaining operational resilience.



Learning from past mistakes:
5 Tips for effective board reporting

Below are my top pitfalls and tips on how to prepare and present to the board.

1. Do not educate — or report to — the board: Genuinely interact with the people on the board rather than merely educating or reporting to them. These sessions are not just for presenting to the board but also for the CISO to understand the board's expectations by hearing them directly.

2. Provide a simulation to promote knowledge-sharing and engagement: Use tabletop exercises not only to impart knowledge but also to grasp the board's expectations. As a CISO, you will probably learn as much as the board members themselves, so you can update your incident management playbooks accordingly. Again, a board presentation is a two-way street.

3. Start with the one thing you want the board to take away: Do not assume that you will have a lot of time with the board. During my last five years as a CISO, I had very few hour-long slots. More typically, I would have 10 minutes to make my points. The board may or may not review your material beforehand but regardless, it's a good idea to start with the one thing you want the board to take away from your presentation and be sure to align that message with the board's priorities.

4. Focus on the business context and very few KPIs: Very early on, I had metrics for everything, up to the point where I had over 100 different KPIs. The board told me that they could not see the wood through the trees, so I scaled those down to 10 KPIs. Even then, it's not always about what information you're sharing but how. For example, I once shared a KPI that said 2% of our servers were unpatched, which was effectively meaningless to them without business context. I clarified that the payment systems were exposed to a critical vulnerability, and if compromised, we could lose our ability to make payments. They then understood the message much clearer.

5. Work with a board member before the meeting (if you can): I was lucky to have been allocated a member of the board who helped me prepare for the meeting. That board member did not have deep knowledge of cybersecurity but helped me anticipate some of the questions and concerns others might raise during my presentation. As a result, I was better prepared and delivered far more value to the business.

Boards have ultimate accountability for all risks and are tasked with determining the level of cybersecurity risk their organisations are prepared to accept. By incorporating these actionable tips, CISOs can navigate board interactions more effectively, fostering better communication, understanding and strategic alignment.

About the author:

Jason Mallinder

Jason Mallinder is a client partner at ISTARI. He is the former Global CISO and a Managing Director at Credit Suisse. He was responsible for information security, including cybersecurity and technology risk management, globally. Having joined in 1998, Jason spent 25 years at Credit Suisse and held numerous roles in technology and operational risk during his time at the bank.
Jason is a certified information security manager and certified risk manager. He chaired the Investment Banking Information Security Group in the U.K. and works closely with the Bank of England and U.K. government on cross-sector cyber defence development, testing and exercising programs.