Reporting to the Board: A Best Practices Guide

By the Trellix® CISO Council

Table of Contents

Introduction: CISOs and the Board

You finally have a seat at the table. Now what?

For many CISOs, reporting to their organization's board is a relatively recent phenomenon. In the past, it may have been the head of compliance or risk who reported to the Audit Committee, with information from the CISO (or CIO) constituting a fraction of that report.

This has changed. Cybersecurity has grown in importance as both cybercrime and regulatory pressure have increased. In the U.S., the Securities and Exchange Commission ruled publicly traded companies must report on cybersecurity in their annual filings. These disclosure requirements are creating more visibility and opportunity for CISOs to have a seat at the table.

Once you have a seat, what do you want to say? A well-crafted board presentation will not only help your organization be better prepared against cyber risk, but it can also enhance your long-term career growth. The opposite can lead to what one CISO euphemistically referred to as a "resumé-generating event."

Preparation is critical. This guide is based on best practices sourced from the Trellix CISO Council. These seasoned leaders have shared their own experiences to help you maximize the impact of your time in front of the board. These general guidelines should help anyone who wants to increase their effectiveness in reporting to a board of directors, but bear in mind every industry—and organization—is different. Use them or adapt them according to what makes sense for you.

Board Reporting by the Numbers

How much time CISOs have in front of their boards varies. For some, it's a half-hour every quarter. For others, it may be a few minutes a couple of times a year. In recent Mind of the CISO research of 500 global CISOs, 49% revealed they were reporting to their board as frequently as once a week. Factors such as your industry, regulatory landscape, and whether you've had a recent attack or incident will affect how much time you spend with your board.

A report to the board represents a much-needed opportunity for alignment—an area some CISOs find challenging. Consider that 59% of nearly 300 global CISOs surveyed feel their views are misaligned with those of their CIO/CEO. Their top 3 reasons:

51%	The CEO or CIO views cybersecurity as a cost center rather than a value driver
46%	Struggle with effective communication
41%	Lack of cybersecurity understanding

Source: Mind of the CISO: The CISO Crossroads

Part 1: The Transformational CISO

As your career evolves, expect to take a more consultative, business-focused approach.

The CISO role has evolved significantly since Citi hired the first CISO in 1995 to deal with information security risk. Roughly 30 years later, many CISOs find themselves at a crossroads where they face competing priorities, including increased regulatory compliance burdens and more time in front of the board. In our "Mind of the CISO" research, 84% of those surveyed supported the idea of splitting the CISO function into separate technical and business-focused roles.

CISOs who seek to grow beyond technical and infosec expertise are poised for transformational leadership in their organizations by educating and guiding their boards on reducing risk in cybersecurity. The transformational CISO has gained the board's confidence and speaks to the board in a language it understands. You're able to communicate your program's successes, educate other leaders on risk, report on the results of investments, and gain support and budget for new investments.

What separates a transformational CISO from the rest? It comes down to mastery of three critical skill areas—architect, operator, and connector. A board report presents the opportunity to show off all three skills.

Architect

Being an architect means being a domain expert with deep technology skills and an ability to fuse business and technology priorities.

Operator

To be an effective operator, you'll need to speak the language of your business and unite it with an understanding of what's going on in the world.

Connector

Think communication, social capital, and soft skills. A connector can effectively communicate the story of risk, ultimately gaining the board's confidence and further investment.

> **"You have to tie everything back to business objectives. It's not really security they want to hear about, as much as revenue protection and business risk."**
>
> –Everett Bates, CISO, Crunchyroll

Part 2: Anatomy of a Board Report

When constructing your board report, think in terms of investments instead of incidents.

Many CISOs—especially those early in their careers—report feeling a lack of alignment with more business-focused leaders. Members of the board typically have financial and business backgrounds as opposed to infosec or technical experience. They may see cybersecurity as a cost center rather than a value driver. Your presentation is an opportunity to educate and guide the board on key matters affecting the business.

A Starter Board Deck

For a quarterly report, include these elements.

- **How you've structured your organization:** Show the operating model in your department with an overarching organizational map and then align a slide to each function. This section of your presentation might include:
  - Who's on your leadership team
  - Programs
  - Governance, risk, and compliance (GRC)
  - Security operations
- **Program updates:** As a rule of thumb, include one or two slides per program. At a public company, your programs (such as GRC) might have subprograms or initiatives that each will get a slide. For each, include:
  - A short description or summary
  - Risk posture and vulnerabilities
  - Key metrics with a description of what they refer to and context
  - Business outcomes achieved over a defined period of time

Part 2: Anatomy of a Board Report

A Starter Board Deck (cont.)

- **Notable attacks or incidents:** Cover only the most important incidents.
- **Achievements and successes:** Call out what has gone well and explain the success in terms of business impact.
- **Roadmap for what's next:** Highlight your objectives for the next quarter, half, or year with a timeline.
  - Are there new regulations or compliance requirements on the horizon?
  - What is the risk outlook for your business or industry?
- **Appendix:** Include any information the board should be aware of or will want to refer back to.

Reporting on Cybersecurity as an Investment
Remember: Your cybersecurity program is an investment, and the board wants to understand its performance. What has been achieved as a result of these investments? Is it what you've expected (and if not, why not)? Are there any areas that need more investment—or less?

Thinking about your presentation in terms the business understands—such as business risk and investment performance—can help you focus your report on what matters to your audience.

> **"The emerging role of the CISO is to seamlessly connect business and technology teams, ensuring that while data fuels business innovation, it remains protected at every step."**
>
> –Jim Jenkins, Vice President of Information
> Security and Information Security Officer,
> Vantage West Credit Union

Part 3: Presentation and Storytelling

Soft skills make the difference for transformational CISOs.

Putting together a great deck is just one part of your board report. Board presentations lean into the Connector part of the CISO role. As you gain experience and ascend the career ladder, you'll want to develop your soft skills, such as being able to tell a story and read the room.

A transformational CISO is able to present confidently, educate listeners, and present succinctly. You want to speak to your slides without getting bogged down in details and without losing your audience's attention. Your objective is to gain the board's confidence and buy-in—you do that through your delivery, your focus on business enablement, and your storytelling skills.

12 Connector Attributes

Many CISOs who have come up through IT or have deep technical knowledge need to develop their Connector persona. How confident are you in your mastery of the following? Consider how you can add more, either through practice, coaching, or organized activities like classes.

- Public Speaker
- Facilitator
- Problem Solver
- Leadership
- Communicator
- Storyteller
- Collaborator
- Enabler
- Emotional Intelligence
- Educator
- Strategic Thinker
- Learner

Part 4: 10 Best Practices

These CISO-tested best practices will help you make the most of your time in front of the board.

1 Tailor your report for a business audience

This first piece of advice may be the most important according to our CISO Council members. Board members typically have financial or business backgrounds, as opposed to infosec experience.
For best results:

- Don't use acronyms
- Avoid cybersecurity jargon
- Speak in a language the business audience understands
- Don't be too technical
- Read the room and move at a pace that makes sense (e.g., don't get stuck on one slide for too long if you don't have much time to cover other more important topics)

2 Save the details for an appendix

CISOs need to communicate risks to the business, but finding the right level of detail can be challenging. CISO Council members recommended keeping the presentation high-level but backing it up with supporting documents. Every organization is different, but your appendix might be 20 slides or more offering a deeper dive.

3 Make metrics meaningful

Metrics are important, but you want to use them judiciously in your report. Rather than overwhelm your audience with numbers, focus on the ones that have an impact. Always give context so people who are not infosec experts can understand what the metric indicates. For example, for each of your program slides, you might include a handful of key indicators with context explaining:

- What the metric is
- How it's tracked
- What its purpose is
- What the status is
- What direction it's trending
- How it compares to previous cycles

4 Polish your report for visual appeal

You want your report to be easily scannable and visually appealing. Don't crowd the slides with text and numbers. Do include color coding (red, yellow, green), charts, and screenshots. Some of our CISO Council members work with their marketing departments on their reports to make sure their slides are polished and compelling.

Part 4: 10 Best Practices

5 Talk about risk in business terms

Help your audience understand the implications of cyber threats in business terms. You can add tremendous value as a CISO by translating cybersecurity risks into business impacts such as brand reputation, revenue protection, and operational disruption. Increasingly, CISOs are gaining a voice in informing risk decisions.

6 Align to business objectives

Cybersecurity is often seen as a cost center or a source of friction that impedes worker productivity. Think about how you can help the board see the connection between your programs as a CISO and the objectives the board wants to achieve. Wherever possible, align your initiatives with those of the business so you're seen as enabling the business and look for win-wins.

7 Don't read your slides

if the board hasn't had a chance to review your slides in advance, resist the temptation to read the slides to them. The board members can read them for themselves. You want to summarize what's less important so you can call their attention to what really matters.

8 Socialize your report ahead of time

You want to be sure there are no surprises when you present to the board. CISO Council members recommend socializing your report ahead of time. Gather input from your CEO and CIO—along with any other board members you've built relationships with. If a board member has an interest in cybersecurity, ask for their feedback. Having allies who are familiar with your report ahead of time will make for smoother sailing when you are in front of the full board.

> **"My role is to be the chief interpreter. I'm trying to be more tied into the business discussions. Many of us fail to make that switch because we don't speak business, we speak tech."**
>
> –Eric Freeman, CISO, Leidos QTC Health Services

Part 4: 10 Best Practices

9 Build relationships with other board members

Many board members sit on multiple company boards and have deep industry experience. You should be prepared to understand where they're coming from and their frame of reference. In particular, get to know:

- Their background and professional experience
- Where else they serve as board members
- What has occurred at those other organizations or in your industry
- What they care about most

Connect with board members ahead of time and find out if anyone has an interest in cybersecurity.

10 Rebuild trust and confidence when there's bad news

If there's been an attack or other significant security event, expect to face some probing questions. You will need to clearly explain what happened, what the impact was, whether the threat has passed, and what you are doing to prevent it from happening again. These sessions can be uncomfortable, but transformational CISOs can approach them in the spirit of deepening trust with the board and driving discussions about resiliency. Many CISOs report they've received more support and investment from the board after an attack.

Part 5: Serving on a Board

As the role of the CISO evolves, CISOs are becoming comfortable interacting with the highest levels of the organization. Many CISOs see serving on a board as part of their career path.

Here are some recommendations from the CISO Council:

Further your business education

Most CISOs come from a technical rather than a business background. Consider how you can expand your business education, whether that means gaining additional training or going back to school.

Think about the value you can bring to a board beyond cybersecurity

You don't need to be an expert in everything, but you should expect to be able to give input on the majority of business that comes before the board.

Find ways to get started

CISO Council members recommend looking at nonprofits or other advisory boards as a way to get your first board experience. Try a board-matching service to see what's out there.

> **"In our sector, we're trying to drive the conversation away from [security] controls. Controls are our problem, not the board's problem. The board's problem at the end of the day is actually what matters, which is resilience."**
>
> –Rob Labbe, CEO & CISO-in-Residence,
> Mining and Metals ISAC

Part 6: Resources

Our CISO Council discussions are meant to share knowledge and help CISOs better protect their organizations while growing their careers. Explore these resources as part of your CISO journey:

Get to know the CISO Council

View our CISO resources

Read The Mind of the CISO: CISO Crossroads report

Check out the book recommendations that came up in our board reporting discussion:

Reframing Organizations: Artistry, Choice, and Leadership

How to Measure Anything in Cybersecurity Risk