Barracuda

Your journey, secured.

The CISO script: How to talk to business leaders about security risk

Cyber resilience is not just about having the right security measures in place. It's about how these measures are implemented and governed. The newly updated NIST Cybersecurity Framework (version 2.0) recognizes this by adding governance as an overarching strategic goal, alongside the ability to identify, protect, detect, respond to, and recover from an incident.

Security is governed by business leaders, senior managers, executives, and the board. Many of them will not have a security or even a technology background, but they will somehow need to understand the cyber risks the organization faces and how to manage and mitigate them.

There is no one-size-fits-all way of explaining security risk to business leaders. No two people or organizations are the same. Each has their own culture, history, expertise, perceptions, and appetite for risk.

For a CISO to effectively protect the company and its assets, they need to know how to engage and involve these disparate groups and individuals in the security conversation.

This is what works for me.

Riaz Lakhani, CISO, Barracuda Networks Inc.

Know your stakeholders

First and most importantly, you need to understand the knowledge and experience that other people bring to the table and what they need and want to hear from you.

What is their role and responsibility, their background, and how would a cyber incident impact their division and their team?

Security is not a one-person job. A CISO needs to be able to get people who don't work for them to do work for them. This means that you need to be able to influence people at all levels in the organization and help them to understand and engage with security policies, incident response, and more.

The time spent listening to and learning about your key stakeholders is one of the best investments you can make. It should guide the language and concepts you use to talk about security.

The closed-door office conversations

It is important to have a regular cadence of meetings with the most senior stakeholders, covering critical risk areas such as engineering, finance, and legal. These scheduled conversations should look at how things are evolving in the threat and security landscape and what this means for the business roadmap, regulatory compliance, supply chain security, and more.

I have a monthly CEO security readout that brings together the CEO, General Counsel, and Chief Financial Officer. I also hold regular one-on-ones with the other executives. We review their part of the business through a security lens. How might their team better support or implement security, where are the gaps, where is the friction, and how do we fix that?

The watercooler chats

Personal relationships sit at the heart of a CISO's success. Every two months I clear my schedule and just talk to people. Salespeople, engineers, developers, security researchers. We talk about anything and everything. It helps me to see the business and security from others' perspectives.

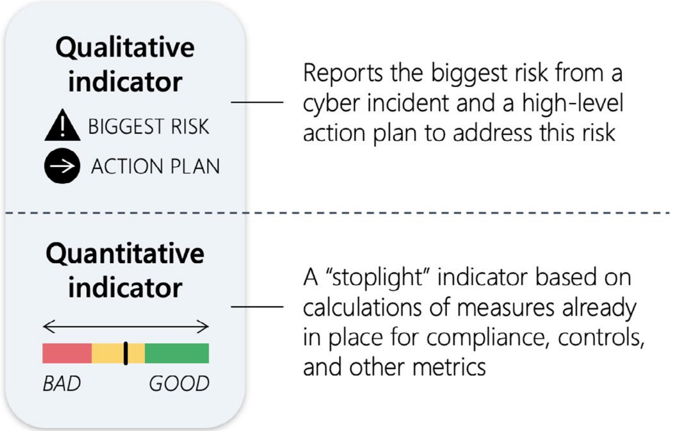
You need to invest in these relationships. If someone doesn't know you and you don't know them, then they're not going to take your call at 2 a.m. And in our line of work, the chances are that sooner or later you will need to call someone at 2 a.m. and ask for their help.

Taking it into the boardroom

Every board is different, but there are a few strategies that work for everyone.

1. **Prepare properly** — Learn what you can about the people around the table and make sure your slides speak to them in a language and concepts they will understand. You don't need a 100% match, but you do need to ensure everyone will be catered for somewhere.
2. **Identify the 'North Star'** — What is the key to capturing your board's interest and attention? Is it about the impact of a cyber incident on brand reputation, risk, regulations, financial return on investment (EBITDA), metrics and numbers, or any combination of these? Is it about cyber resilience, and how we can keep the organization resilent in a world where cyber incidents are common, unpredictable and potentially destructive? Use this to frame your story.
3. **Less is more** — Keep slides and their content to a minimum. Visualize as much of the information as you can. It helps to remain consistent in your approach and format from one board meeting to the next, so that people know what to expect and can easily track progress and change.
4. **Find your cyber ally** — This is someone on the board who knows about cybersecurity and who you can share ideas and thoughts with before the meeting. They will be in the room to support and reinforce your narrative and help you navigate your way through.

We are fortunate to have Keri Pearlson on our board here at Barracuda. Keri is the executive director of the research consortium Cybersecurity at MIT Sloan (CAMS). Her independent insight and counsel are invaluable. Keri is also the creator of the Cyber Resilience Scorecard, a powerful visual tool to help businesses measure their cyber resilience.


Qualitative indicator
⚠ BIGGEST RISK
→ ACTION PLAN
Reports the biggest risk from a cyber incident and a high-level action plan to address this risk
Quantitative indicator
BAD
GOOD
A "stoplight" indicator based on calculations of measures already in place for compliance, controls, and other metrics

These scorecards enable you to share essential facts and metrics with the board in key areas of risk or strategic focus. Further details on how to use these can be found in the Harvard Business Review and in our template CISO deck that's available to download.

Maintaining momentum

Alongside the conversations, readouts and board presentations, a good way to keep your key stakeholders engaged with the language of cybersecurity is through regular tabletop cybersecurity exercises.

A tabletop exercise is a simulated cyber incident, minus the actual damage, impact, and cost. The most effective tabletops are controlled, scenario-based exercises where key stakeholders, such as IT personnel, security teams, business and functional leaders, come together to work through and evaluate their combined response to a hypothetical security incident.

Quarterly or biannual exercises provide a valuable opportunity to test your incident response plan, identify weaknesses in specific areas, build awareness of the potential impact of specific threats such as ransomware, supply chain security breaches, and more.

Barracuda assets for CISOs, CIOs, and other technology leaders

The following assets are available to help organizations of all sizes to better understand, manage, and measure their cyber resilience.

- Presenting cybersecurity and risk to the board
- Leading the business to cyber resilience
- The cyber resilience check list
- Securing tomorrow: A CISO's guide to AI in cybersecurity