Balbix®

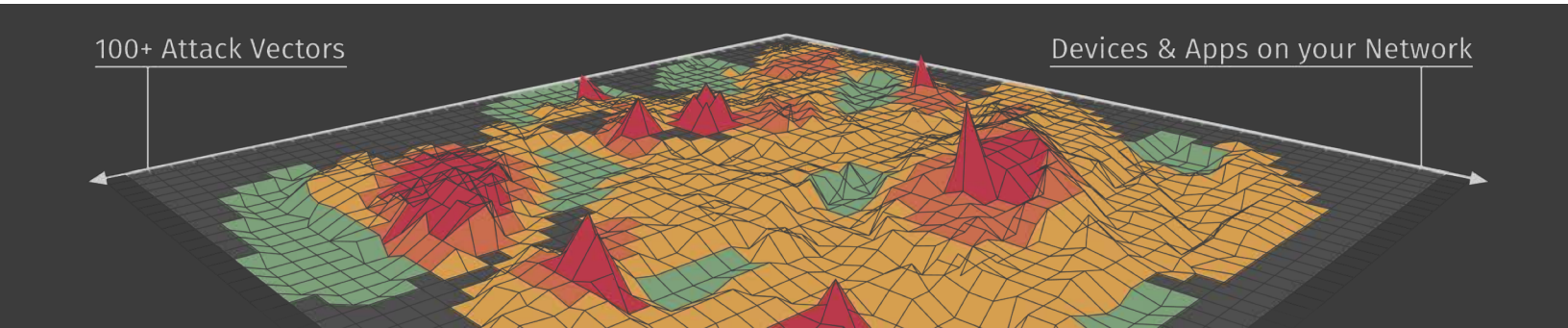
3 Success Factors for Cyber-Risk Reporting to the Board

Balbix®

The board of directors is responsible for seeing that a company steers a safe course as it delivers on its mission. Because the board oversees strategic and operational decisions, it is important that members have a very clear picture of business risks as they work to ensure that profits are maximized, and legal and regulatory obligations are being met.

Thanks to several highly publicized and costly breaches, cybersecurity is one of the top board-level concerns. Breaches negatively affect a company's reputation, customer experience, and bottom line. That said, board conversations about cybersecurity are difficult because it's a complicated subject. The enterprise attack surface is massive, there are many moving parts, and the places where things can go wrong are too numerous to count.

Also, board members and c-suite executives are big picture thinkers, so this very complex topic needs to be presented in a way that makes sense to them. In short, you need to "speak their language" as you communicate cybersecurity posture, risks, and recommended actions to your board. Here are 3 success factors to keep in mind.



01

Quantifying Cybersecurity Posture

Cybersecurity posture is an aggregate of the strength of a company's cybersecurity policies, safeguards, and controls, and how effectively they mitigate risk. In an ideal world, you would be able to compute a simple risk score for your enterprise that shows where your cybersecurity posture stands at any point in time and how you compare against peer organizations. You would also be able to tie security vulnerabilities to business criticality so that you could prioritize actions and tackle the most serious risks first.

01

But where do you begin? How do you quantify the size and scope of the problem?

What is the best way to discuss cybersecurity posture and recommended actions with board members and c-suite colleagues? Here are some key ideas to keep in mind.

- You need to redirect conversation from cybersecurity to cyber-risk but stay tied to actual on-network cybersecurity posture.
- You must identify key areas of the business at risk from cyber-attacks, and help your colleagues understand how your cybersecurity program is aligned to this risk.
- At the board-level it is all about benchmarks, so you must be able to compare your security posture and breach risk to similar organizations. Your board will expect you to recommend appropriate level of residual cyber-risk your organization should aim for.
- You must have internal benchmarking data - what is working well, and what is not. And which groups have good cybersecurity posture vs ones that don't.

Balbix®

01

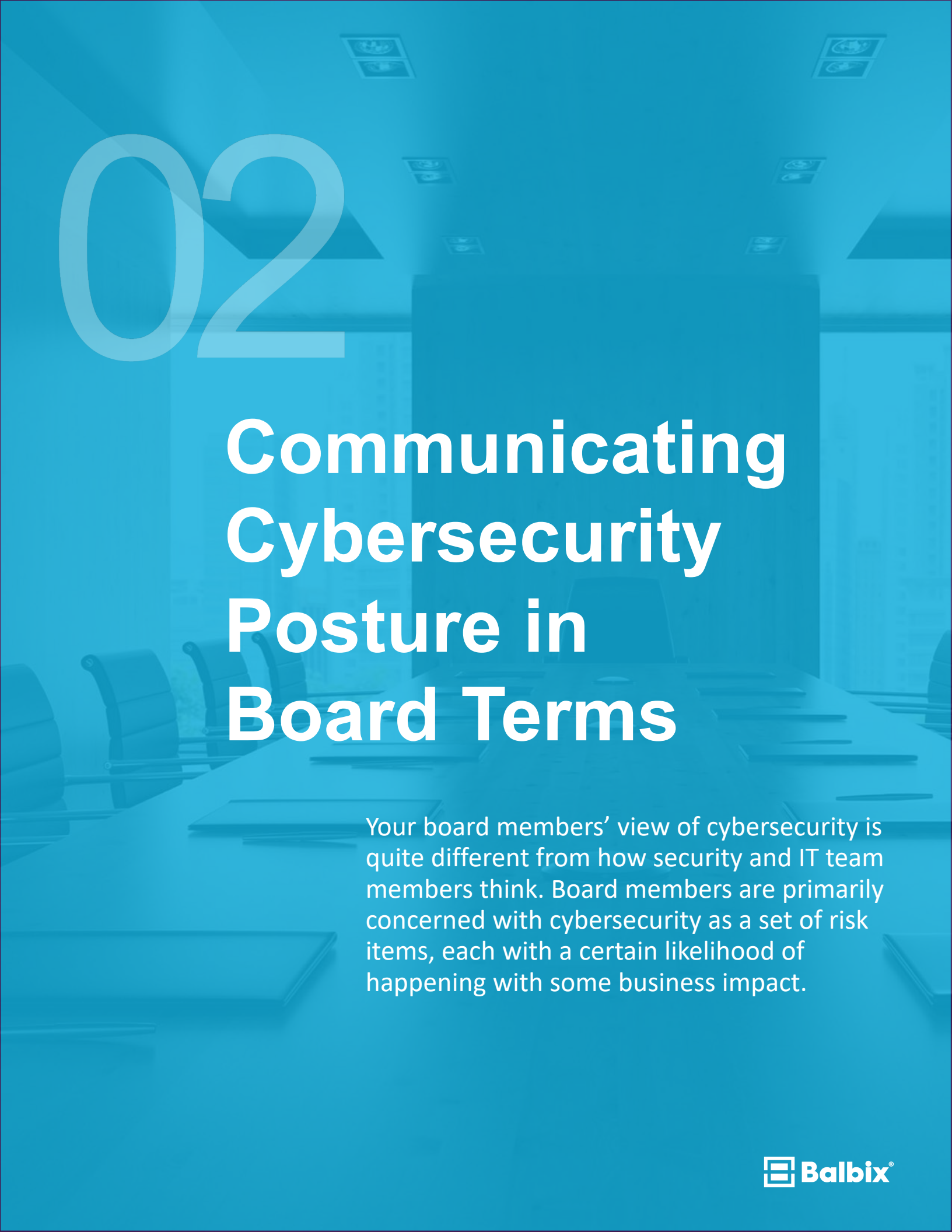
How Balbix can help

Balbix analyzes your attack surface inside-out and outside-in to give you a 100x more accurate view of breach risk than any other method. The foundation of cybersecurity posture quantification is visibility which starts with an accurate inventory of your assets, understanding and prioritizing risks to those assets, and implementing appropriate controls to protect them. Armed with this visibility into everything that needs to be protected and in what priority order enables you to help your board understand how cybersecurity posture is aligned to cyber-risk.

Balbix®

Good cybersecurity posture reporting needs to be simple, quantitative, aligned with business risk both externally and internally, and backed by a plan.

Balbix®



02

Communicating Cybersecurity Posture in Board Terms

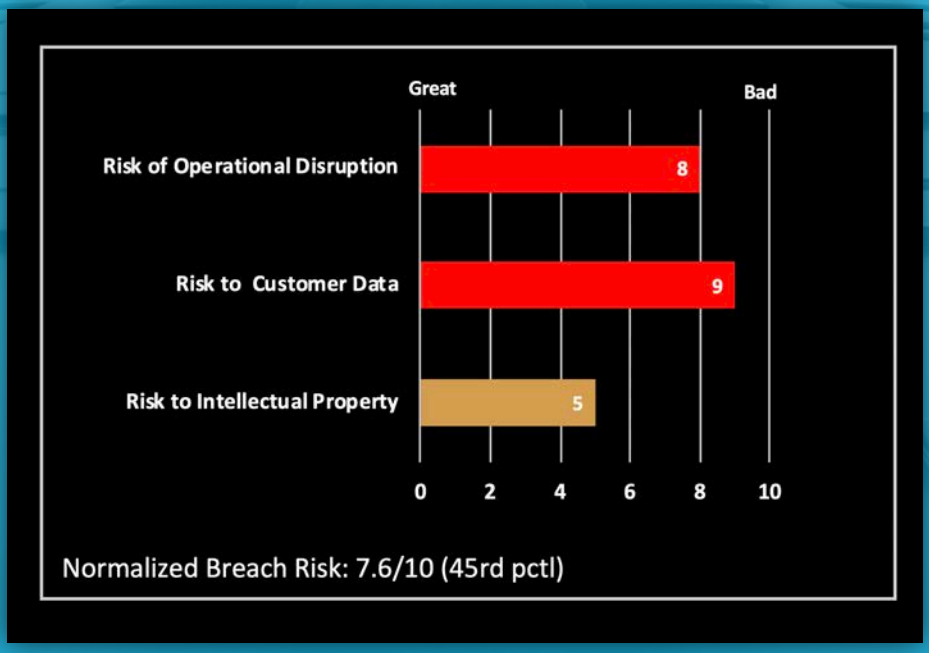
Your board members' view of cybersecurity is quite different from how security and IT team members think. Board members are primarily concerned with cybersecurity as a set of risk items, each with a certain likelihood of happening with some business impact.

Balbix®

02

How Balbix can help

- Internal benchmarking and the risk heatmaps show you the groups of assets that are driving your risk metric. With internal benchmarking information, you are able to show your board and executives how risk is distributed in your organization, which teams, processes, and systems are major contributors, and the types of activities necessary to remediate these risk items.



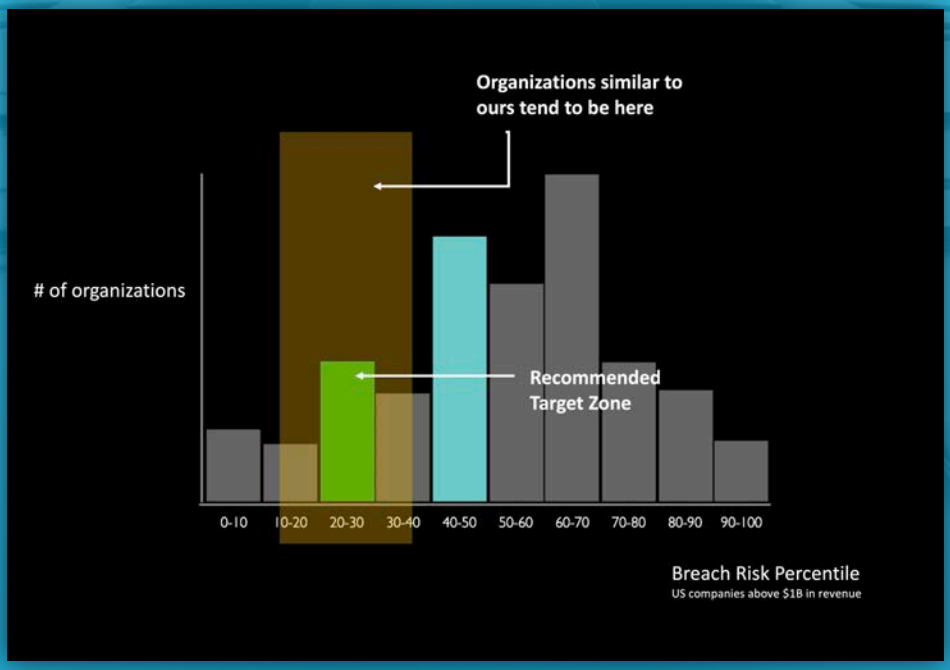
Cyber-risk metrics aligned to business concerns

Balbix

02

How Balbix can help

- External benchmarking shows board members and executives the level of acceptable risk that is appropriate for your organization. Comparison with peer entities is a common method which senior leaders use to grade performance. Balbix helps you benchmark your security posture against similar organizations and use this information to help the board understand your cyber-risk goals for the enterprise.



Cyber-risk benchmarking

Balbix

03

Data-backed Execution Plan

Once the board understands current cybersecurity risks, they expect you to have a well thought out execution plan to transform your organization’s cybersecurity posture.

Balbix®

03

How Balbix can help

Balbix prescribes prioritized actions that you can take to improve your network's cyber-resilience and decrease breach risk. The platform also provides you with simulation tools that allow you to compare the effectiveness of different remediation plans. In addition, we offer:

- Trends and reporting to show the risk reduction over a particular time period, continuous risk heatmaps with stunning visuals, as well as an automatic and continuous risk assessment, comprehensive risk measurements, and actionable insights across your entire attack surface.
- Visualization of your multidimensional attack surface for communicating with your board, as well as other functional areas across the enterprise.

Balbix®

Recommended reading

Balbix