SOLUTION BRIEF

Cyber-Risk Reporting for Your Board of Directors

Balbix®

Cyber-Risk Reporting for Your Board of Directors

Overview

How should you quantify cybersecurity posture for your board of directors and C-suite colleagues?

As you know very well, your board members' and senior executives view of cybersecurity is quite different from how security and IT team members think. It can be quite frustrating to try to explain advanced malware or technical controls to these folks, most of whom are not savvy about the technical details about cybersecurity. Instead your board members and non-technical senior executives think about cyber-risk as yet another business risk item to be understood and managed.

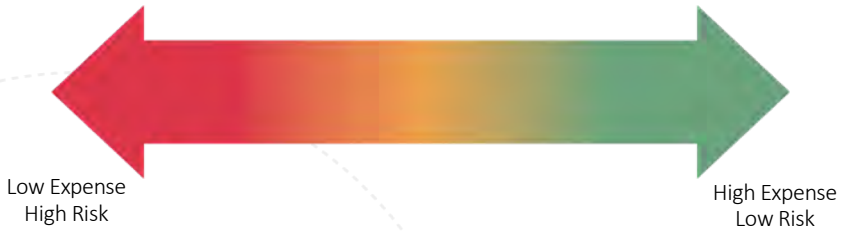

Figure 1: Cyber-risk spectrum

Figure 1 shows a continuum of cyber-risk posture from a board member's perspective. Boards and senior executives have three main questions about cybersecurity and breach risk:

1. Where is the organization on the cyber-risk spectrum?
2. Where should the organization be?
3. How can the organization get to where it should be?

Unfortunately, due to the massive size and complexity of the enterprise attack surface and the practically unlimited permutations and combinations by which the adversary can carry out a cyberattack, you know how difficult it is to analyze your overall cybersecurity posture and calculate your organization's breach risk.

Furthermore, because of this vague understanding of security posture, you and your colleagues struggle to agree on where in the spectrum your organization ought to be, i.e., to agree on when cybersecurity is "done" for your organization.

Your board wants to know ***where the enterprise is*** on the cyber-risk spectrum, ***where it should be***, and ***how it's going to get there***?

Sometimes, these conversations get heated with various people expressing their opinions.

You are not alone if you struggle in your cybersecurity conversations with your board and senior management. In a recent survey conducted by the Ponemon institute, only 9% of security teams felt that they were highly effective in communicating cybersecurity risks to their board of directors and C-suite colleagues.

How can we do better?

Only 9% of security teams feel they are highly effective in communicating cybersecurity risks to C-suite and boards

Elements of good cybersecurity reporting

How exactly should you quantify cybersecurity posture for your board of directors and C-suite colleagues? Here are some key ideas to keep in mind.

1. You need to ***up level the conversation*** from cybersecurity to cyber-risk, but stay tied to actual on-network cybersecurity posture.
2. 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.
3. At the board-level it is all about benchmarks, so you must have a sound mechanism to ***compare your cybersecurity posture*** and breach risk ***against similar organizations***. Your board will look to you to ***recommend*** the appropriate ***level of residual cyber-risk*** your organization should aim for.
4. You must have ***internal benchmarking data*** in your back pocket– what is working well, and what is not. And which groups have good cybersecurity posture vs ones that don't.
5. Your report must be ***backed by a plan***– on how you would change the organization's cybersecurity posture to the recommended level. You will need to explain what you need from the board to execute your plan.
6. Last but not least, you will need to execute your plan, and show cyber risk reduction outcomes and other trends in a quarter or two, and forever thereafter.

Your reporting framework should be systematic – you should not have to resort to ad-hoc analysis and building slides by hand before each cybersecurity meeting with the board. Let's dig into the details of each of these highlighted areas and see how Balbix can help you develop a world-class cyber risk reporting framework for your board of directors and C-suite.

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

Balbix overview

Balbix analyzes your organization's attack surface *inside-out* and *outside-in* to give you a 100x more accurate view of breach risk than any other method. Balbix provides a real-time risk heatmap and prescribes a prioritized set of actions that you can take to improve security posture and reduce risk by a factor of 50 or more, while making your security team 10x more efficient.

In order to make this computation possible, Balbix uses deep learning and advanced AI algorithms to continuously and automatically discover, observe and analyze your attack surface across all your assets and hundreds of attack vectors.

Balbix computes a cyber-risk score for your enterprise that shows where you are and how you compare against peer organizations. Besides risk-scoring, Balbix has a number of key features to make it easy for you to do cybersecurity reporting.

Align with business thinking

As discussed earlier, board members are primarily concerned with cybersecurity as a set of risks items, each with a certain likelihood of happening with some business impact. Balbix lets you to define risk areas appropriate for your business using natural language search, and then maps the automatic calculation and tracking of these metrics to your actual on-network cybersecurity posture.

For example, if your organization cares about risk of loss of intellectual property from cyber-attacks, you can type "risk to intellectual property" in the Balbix search box, and then define this as a key risk item for Balbix to track and report. Balbix automatically maps this risk item to the actual on-network attributes that drive it, and continuously observes and analyzes the relevant parts of your cybersecurity posture.

You are also able to report business-level risk metrics, without having to explain the technical details of your cybersecurity program (Figure 2).

Figure 2: Cyber-risk metrics aligned to business concerns

External benchmarking

Balbix helps your benchmark your security posture against similar organizations, and use this information to help the board understand your recommendations for cyber-risk goals for your enterprise.

For example, you can show the percentile of breach risk that your organization falls in, and where organizations similar to yours are placed (Figure 3). If your enterprise has a mature cybersecurity posture, you are "done", and it is just a matter of maintaining your current level of cybersecurity preparedness. More likely though, you will have work to do and this type of benchmarking can be useful in helping you justify to your board and senior colleagues the need to do this work.

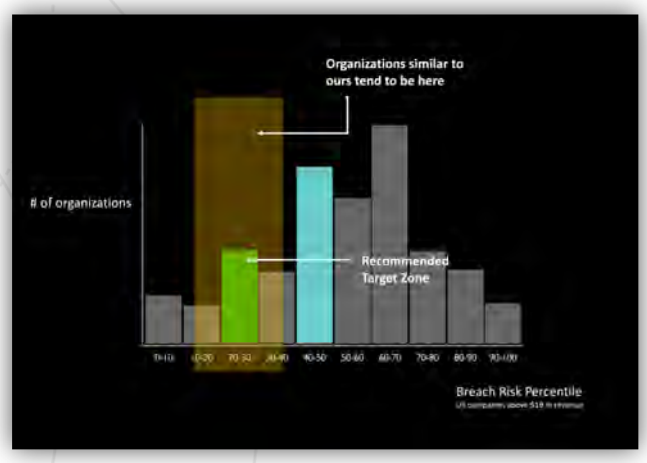

Figure 3: Cyber-risk benchmarking

Internal benchmarking and risk heatmap

In order to improve your security posture, Balbix enables you to drill down from a business-level risk metric or score that you have defined into a risk heatmap which shows you the groups of assets that are driving the risk metric.

With internal benchmarking information, you are able to understand and show to your board and executives necessary how risk is distributed in your organization, which teams are most behind driving the greatest risk. You can also see and explain the types of actions necessary to remediate these risk "bubbles".

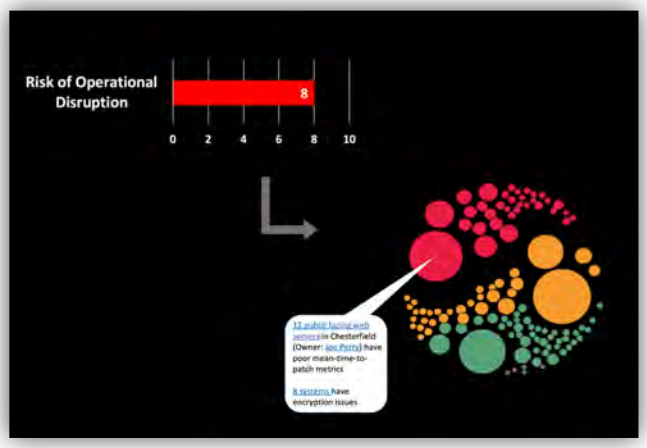

Figure 4: Internal benchmarking

The Plan

Your board expects you to have a well thought-out execution plan to transform your organization's cybersecurity posture to the recommended risk level. Showing up to a board meeting to raise an issue but without a plan is career-limiting.

Balbix prescribes prioritized actions that you can take to improve your network's cyber-resilience and decrease breach risk. This action plan has been back-solved from the hyper-dimensional risk calculations that were performed to analyze your cybersecurity posture. Balbix also provides simulation tools that allow you to compare alternate plans.

Figure 5: Cyber-risk reduction plan

Trends and Reporting

Of course, the next quarterly cybersecurity review with the board comes along soon enough, and you will need to produce slides which show the risk reduction your team has been able to achieve in the last 90 days. Balbix allows you to generate your board slides quite literally by hitting a button, and without any manual heavy-lifting. You do not have to ask your subordinates for various reports, and do not need to spend hours doing painstaking work to interpret these reports and do the necessary manual slide-work.

With Balbix, you can also show trends over 90 days, 6 months, year-over-year or any custom period. The backup security data you need to explain any metric or trend is all there – you can click to drill down and create another slide. You are also armed with all the information you need to answer any probing questions.

Figure 7 summarizes the unique capabilities of Balbix for cyber-risk reporting.

Figure 6: Trends and reporting

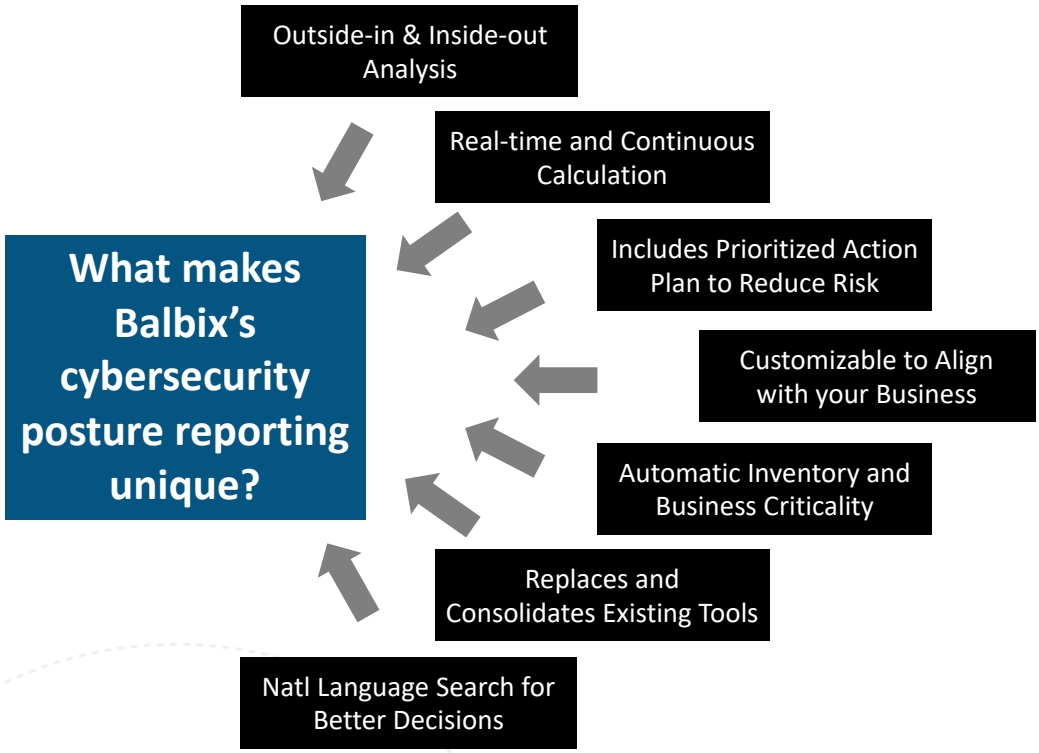

Figure 7: What makes Balbix's cyber-risk reporting unique

Summary

We have entered an era where cybersecurity is no longer a human-scale problem. Quantifying cybersecurity posture for non-technical stakeholders is not an easy task. With Balbix's cyber-risk reporting capabilities, you are able to help your board of directors do their critical oversight job better, and get their support and funding for the necessary security initiatives.

Please contact us at info@balbix.com or click here to schedule a demo to see how we might be able to help.

Help your board do their oversight job better and get funding for your security projects!

3031 Tisch Way, Ste 800
San Jose, CA 95128
866.936.3180
info@balbix.com
www.balbix.com