ULTIMATE GUIDE

Cyber risk reporting to the board of directors

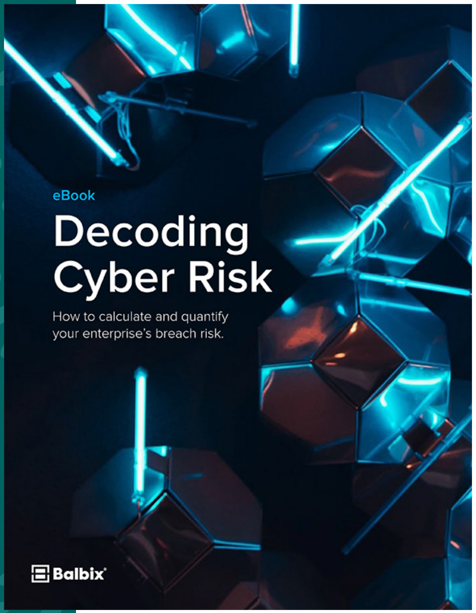
Balbix®

Only 9% of security teams feel that they are highly effective in communicating security risks to the board and to other C-suite executives, according to a recent survey conducted by the Ponemon Institute.

As a CISO, it can seem as though it is impossible to effectively explain and report the importance and workings of the organization's cyber-risk program to an audience that views cybersecurity as yet another difficult to understand, technical topic. As a result, many board and C-Suite decisions related to security are made with gut feelings and with insufficient data.

If you place yourself in the board's shoes and clearly communicate and quantify overall cyber risk, your message is better received, and you are more likely to get the support needed to transform your company's cybersecurity posture.

Learn more about how to mathematically quantify cyber-risk



eBook

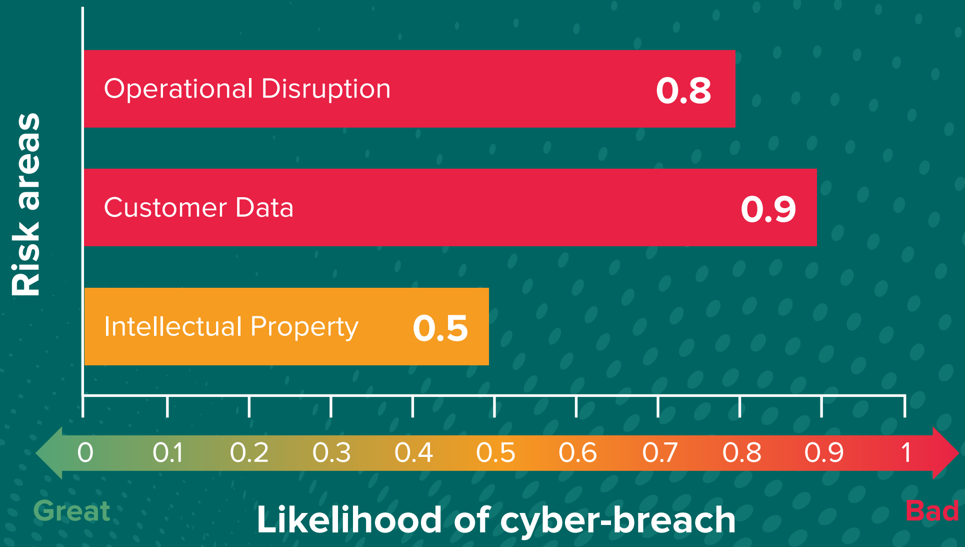
Decoding Cyber Risk

How to calculate and quantify your enterprise's breach risk.

Balbix

Approaching cybersecurity through the board of directors’ perspective

You must reconsider your communication approach and perspective prior to a board and/or C-Suite discussion. Your board members’ view of cybersecurity is different from security and IT team members. From a board member’s perspective, cyber-risk posture is viewed as a set of risk items with corresponding business impact and associated expense. The board wants to know where the enterprise is on the cyber risk spectrum, where it should be, and, if there’s a gap, how it’s going to close it.



Quantifying cybersecurity for the board of directors

Enumerating your cyber-risk and business impact of your cybersecurity measures is no small task, given the massive size and complexity of the enterprise attack surface and the practically unlimited permutations and combinations by which an adversary can carry out a cyberattack. When quantifying cyber risk, there are four key areas to keep in mind.

1 **Identifying the key areas of the business at risk of cyberattack and the current controls in place.** As an example, if your organization prioritizes the risk of loss of intellectual property, you, the CISO, will define this as a key risk item and help your colleagues understand how the cybersecurity program is aligned to managing this risk.

2 **Comparing and quantifying your cybersecurity posture against peer organizations.** It's important to consider that board members and executives are most interested in knowing the level of acceptable risk that is appropriate, and comparison is a common method used to grade performance.

3 **Quantifying internal benchmarking data** will ensure that you are showcasing what parts of the organization's current cybersecurity program are working and what are not. With this data, the board can easily view how risk is distributed in the organization and the teams or areas that are driving the greatest risk. You must present at a high-level the types of actions necessary to remediate key risks to bridge the gap between perceived risk in the boardroom and the actual on-network conditions.

4 **Presenting a plan to achieve the recommended level of cyber-risk and providing quantifiable insights on improvement.** Your plan needs to be converted into an easily digestible, high-level list of small steps or initiatives, each with corresponding time frames, required resources and a dollar cost. Furthermore, given that the board will expect you to drive and execute a plan, you must quantify all the responsible constituents involved. During the next quarterly cybersecurity review with the board, quantifiable improvements that show the risk reduction outcomes your team has achieved over time should be highlighted.

What CISOs say about reporting cyber risk to the board

CISO Focus Group

17 CISOs from public and private companies from a variety of industry verticals including Finance, Insurance, Manufacturing, Retail, and Transportation met. Rounding out the group, we had one CISO from the government sector.

All CISOs, except one, present to board members and/or audit committees multiple times a year. For larger or more security-mature organizations, the cadence is quarterly meetings with the audit committee and semi-annual or annual meetings with the full board. For others, there is no relevant board subcommittee and they present to the full board on a quarterly basis.

Many CISOs in the group (roughly 40%) said that they have spent a lot of time educating their boards about cybersecurity and breach risk and feel that their boards now understand the nature of the beast. Three CISOs were still in the early part of their "educate the board" journeys. The balance of our group was somewhere in the middle.

The persona of the typical board member was very succinctly put into words by one CISO: "accountants or lawyers, primarily concerned about expenditure or liability to the company" and "they don't really know much or care about cybersecurity". This is not surprising given the typical composition of board audit committees and the technical nature of cybersecurity.

Most CISOs spend a lot of time preparing materials ahead of board/committee meetings and providing them to the board members as long as 30 days before the meeting. Some CISOs have found one board member they work with outside the regular meeting cycle to understand new concerns or questions that might be worrying the board.

Four key takeaways

1 Compliance is security

We have all heard CISOs and CIOs on numerous occasions proclaim that compliance is not security. An organization can be completely compliant and yet quite vulnerable to a data breach. Many of the data breaches in the last decade have involved organizations that had passed many compliance-related audits.

Many CISOs in our focus group thought differently on this topic. For them, an organization cannot claim to have a good cybersecurity posture without first attempting to align against and comply with some standards framework. More importantly, these CISOs are trying to drive home to their senior executives and board members that it is impossible to be compliant against any data protection standard unless they also have an appropriately good cybersecurity posture. This is used to drive budget allocation for important security initiatives using compliance dollars.

2 Privacy gets their attention

WCISOs are seeing privacy become a real hot button topic with board members with the advent of GDPR, CCPA and similar regulations. They are beginning to see the board ask to be educated on these topics and informed about the state of "privacy compliance" of the organization. Many of our group's members see this has a huge upcoming challenge in 2020 and beyond that is restricted not just to educating the board but also doing the same for many parts of their organizations. They foresee many difficult discussions that will wrestle with questions like: "what exactly do we do with our customers' data" and "what things can we not do with this data" while "not stopping the business".

Along these lines, 3rd party vendor risk was also front and center for our focus group's CISOs who see many potential bombshells in the yearly/half-yearly checklist-style cybersecurity posture questionnaires provided by their vendors. One CISO indicated that his organization had deployed VDI for key outsourced business processes to prevent any data transfer to a less secure environment.

Four key takeaways

3 There are exceptions

Many of the CISOs acknowledged that issues that fell into their “approved exceptions list” were not reported or discussed with the board. The exceptions list contains all sorts of situations including un-patchable or obsolete systems, missing controls, absent processes, non-compliant 3rd party vendors.

Some CISOs felt very strongly that this was their (very frustrating) Achilles heel—an official mechanism to sweep difficult things under the rug and prevent them from being discussed or reviewed with the board, a growing bubble just waiting to burst.

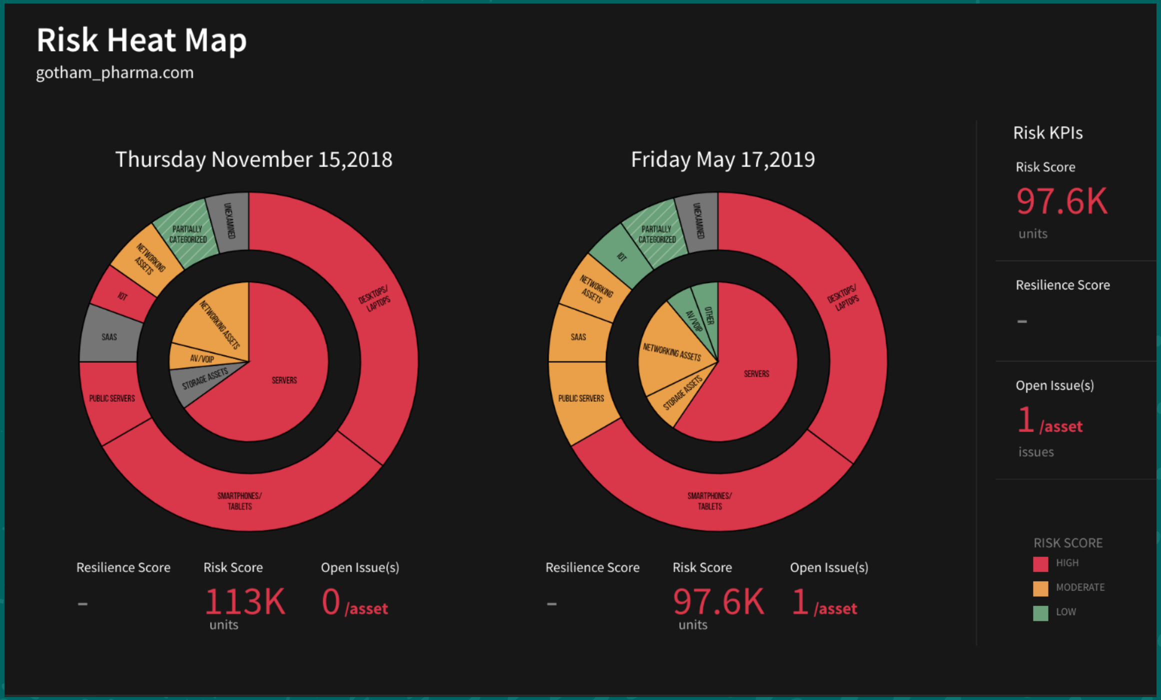
4 Visibility is key

3rd generation cybersecurity technologies are giving CISOs better visibility than they’ve ever had into their security posture. CISOs with adequate visibility were able to answer questions from the board like “How many assets do we have?” and “Where does our customer data lie?”

The CISOs with the best visibility into their attack surface can field questions like “Which of my assets are at highest risk of breach and why?”, “Is our customer data safe?”, and “Are we compliant?” For almost all CISOs, getting real-time visibility and visibility into vulnerabilities beyond CVEs were top priorities.

How Balbix can help

The Balbix platform analyzes your entire attack surface in order to obtain a more accurate view of breach risk, compute a risk score for the enterprise, then compare that score against peer organizations. Not only will this allow for more transparency in the company's security posture, but it will increase the business' security teams efficiency and reduce risk by seeing which actions need to be taken in order to improve your security posture.



Risk Heat Map

gotham_pharma.com

Thursday November 15,2018

Resilience Score -

Risk Score 113K units

Open Issue(s) 0 /asset

Friday May 17,2019

Resilience Score -

Risk Score 97.6K units

Open Issue(s) 1 /asset

Risk KPIs

Risk Score
97.6K
units

Resilience Score
-

Open Issue(s)
1 /asset
issues

RISK SCORE
🟥 HIGH
🟧 MODERATE
🟩 LOW

Understand your attack surface

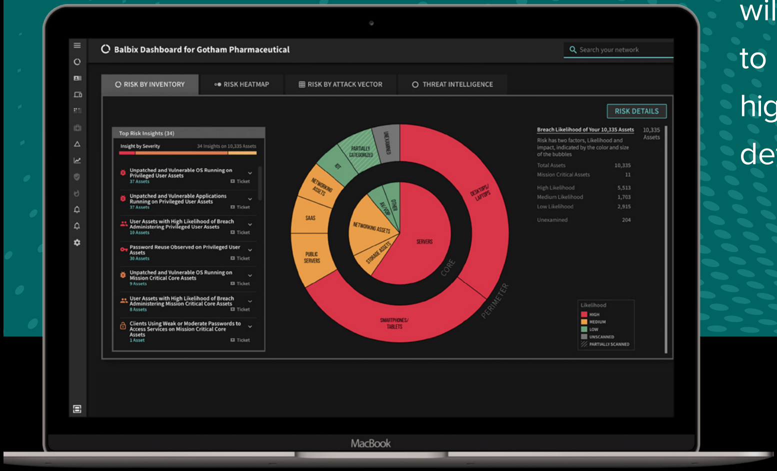
Balbix continuously observes your extended enterprise network inside-out and outside-in to discover the attack surface and analyze hundreds of millions (or more) of data points that impact your risk. Organizations can track their inventories in real-time and stay current on security issues affecting business critical devices, software, and other assets.

Get an accurate read on your risk

Balbix calculates your enterprise's real-time risk, taking into account open vulnerabilities, business criticality, applicable threats and the impact of compensating controls. Analysis of all possible breach scenarios—the various combinations of attack starting points, target systems and propagation paths—and precise determination of the riskiest scenarios is key. This real-time risk model is surfaced to relevant stakeholders in the form of highly visual drill-down risk heat maps and Google-like natural-language search. You can ask questions like "where will attacks start" or "what is the risk to customer data," and get a relevant, highly visual answer, along with drill-down details on how to mitigate the risk.

Obtain prioritized action items with prescriptive fixes

Balbix generates a prioritized list of actions that will affirmably reduce risk. Security posture issues with the greatest risk are addressed first before working down the list of smaller contributors. For each issue, responsible owners for the corresponding assets are identified and then prioritized tickets containing all relevant context are generated and assigned to these owners. Progress is closely tracked and fed back to relevant stakeholders.



Balbix Dashboard for Gotham Pharmaceutical

Top Risk Insights (34)

Insight by Severity 34 Insights on 10,335 Assets

- Unpatched and Vulnerable OS Running on Privileged User Assets — 37 Assets — Ticket
- Unpatched and Vulnerable Applications Running on Privileged User Assets — 37 Assets — Ticket
- User Assets with High Likelihood of Breach Administering Privileged User Assets — 10 Assets — Ticket
- Password Reuse Observed on Privileged User Assets — 30 Assets — Ticket
- Unpatched and Vulnerable OS Running on Mission Critical Core Assets — 9 Assets — Ticket
- User Assets with High Likelihood of Breach Administering Mission Critical Core Assets — 8 Assets — Ticket
- Clients Using Weak or Moderate Passwords to Access Services on Mission Critical Core Assets — 1 Asset — Ticket

Breach Likelihood of Your 10,335 Assets — 10,335 Assets

Risk has two factors, Likelihood and impact, indicated by the color and size of the bubbles

Total Assets	10,335
Mission Critical Assets	11
High Likelihood	5,513
Medium Likelihood	1,703
Low Likelihood	2,915
Unexamined	204

LEARN MORE

Balbix®