



— Why Your Cybersecurity Posture Isn't Working and How to Fix It

Status Quo

It can give Frankenstein a run for his money

Your current security posture is a mish-mash of security point products that you have deployed in your quest to address security “projects”. This project-oriented approach to security is one where teams are focused on completing security projects off of to-do lists without having any real insight into whether or not these projects have a meaningful impact on

your organization’s security posture. This usually involves deploying products from a bunch of different vendors without realizing that:

- A** Each company’s product is actually just a “feature”
- B** The various tools don’t work together
- C** These are all point solutions

What this really means is that your security practices and products are narrowly focused.

It's all about jumping from one fire to the next

Nearly all new security spending and effort is directed toward detecting an attack in progress or responding to one that has already occurred. While putting out security “fires” is an essential practice, the best way to build a secure enterprise is not necessarily by:

- A** Hiring a lot of firefighters (security operations and triage teams)
- B** Purchasing all possible anti-fire equipment (lots of security controls)

What this really means is that your security spending is mostly reactive.

You are trying to fix all the cracks instead of putting away your food to protect it from rats

You are spending most of your spending efforts on fixing indicators of compromise (IOC) alerts, patching, and chasing commitment biases, without really knowing the answers to questions like:

- A** Which of my assets are most critical?
- B** What threats are active right now?
- C** Which of my assets are most vulnerable?

What this really means is that your security posture may not be aligned with how attacks are occurring.


You speak English, he speaks Spanish, she speaks French

Your operational teams such as SecOps understand all technical details and speak “tech”, while your executives and Board speak the language of “risk.” And to add to this confusion, there are different types and levels of:

- A** Reports
- B** Slides and presentations
- C** Dashboards
- D** Metrics

What this really means is that various stakeholders do not share the same language of security.

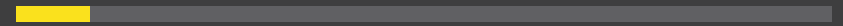
Need stats, facts, and figures?




61% of respondents acknowledged that they don't have adequate context on the business impact if a vulnerable asset got breached.



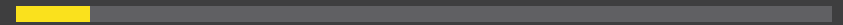
56% cannot predict where or which assets would be compromised.



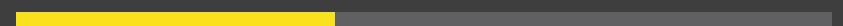
Only **9%** respondents said their organizations have made cyber security a board-level priority.



71% feel that their organization's execs and senior management do not clearly communicate their business risk management priorities to IT security leadership.



Only **9%** feel that security teams are highly effective in communicating security risks to c-suite and boards.



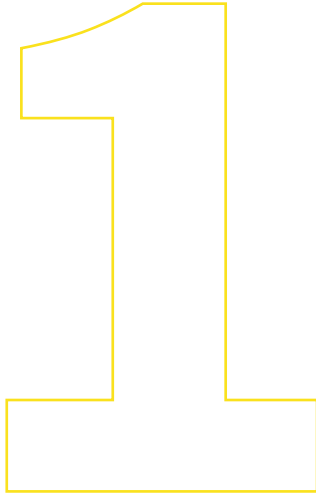
Only **33%** are confident that they can avoid data breaches.

CyberArk Advanced Threat Landscape Report 2018
Ponemon Challenging State of Vulnerability Management Report 2019

Okay, Okay, I Get It. **What Now?**

Leaders like you realize that you can't afford to continue to dedicate time, resources and budget toward fixing problems without having a clear understanding of how those actions reduce the company's overall cyber-risk. Your existing security practices need to be evaluated with a fresh lens to move your cybersecurity posture to a more robust stance. Read on to see what you need to do.





Comprehensively measure the attack surface.

You can do this by first obtaining a real-time inventory of all your IT assets, including managed, and unmanaged servers, laptops, BYODs, IoTs, etc. and automatically discovering any assets newly added to your network in real-time. And then continuously monitoring them across a broad set of attack vectors (unpatched software, phishing and ransomware, misconfigurations, encryption issues etc.)



Result: Continuous, real-time visibility into inventory, vulnerabilities, threats, and mitigations.

2

Meticulously model breach risk and predict breach scenarios.

In addition to discovering and categorizing your assets, it is imperative to calculate the business impact for each asset by examining its access to sensitive networks, services and data. This coupled with the continuous analysis of indicators of risk across dimensions like weak and shared passwords, misconfiguration, susceptibility to phishing, unpatched software, quality of encryption, etc., produce an inherent likelihood model for the network. Then fold information about the external threat model and the deployed security controls and mitigations to compute the effective risk model for the enterprise.



Result: Security practice is now proactive instead of reactive.

3

Perform actions that systematically reduce breach risk.

Obviously, there are specific steps you can take to improve your security posture. But the big question is, how do you know what those steps are, in order of priority, and how to take them? Your action items need to be derived directly from your breach risk model. Then these actions will not just be a sweeping list of vulnerabilities, but the result of analysis of your overall attack surface based on actual risk. Some of these insights will be tactical tasks – one-time fixes, such as “change this password” or “patch that system”, while others may point to some strategic actions, e.g. “the mean-time-to-patch for this set of 25 critical assets is too high. It should be 3 days” or “these set of 150 systems have very high risk. They don’t appear to need unfiltered internet connectivity. Consider firewalling them off with tight network segmentation”.



Result: Security posture is properly aligned with cyber-risk.

4

Make security related information accessible to multiple stakeholders ranging from security analysts to the board.

Recognize that being breached has far-reaching consequences for the organization. This means that responsibility for managing risk belongs to everyone. Educate your board of directors about your security posture and where you are on the cyber-risk spectrum. Inform them regularly about how the actions of the security team result in business risk reduction outcomes, and how the various security projects tie into the goals of the company. It is also important to avoid getting into technical security KPIs and instead, talk about metrics around risk and resilience.



Result: Clear communication at the appropriate levels enables alignment across the enterprise.

Transforming your security posture

Beyond the Status Quo

Balbix BreachControl provides you with a 100x more accurate view of breach risk. Balbix also prescribes a set of prioritized actions that enable you to transform your security posture and decrease breach risk by a factor of 50, while making your security team 10x more efficient.

Balbix BreachControl performs a comprehensive calculation of risk and resilience, continuously observing and analyzing the enterprise attack surface to surface relevant insights for security teams and the business. These insights are used to assist the cyber-security related decision-making process for the enterprise – such that the right mitigation actions are prioritized and executed, and the correct indicators of business risk are used. This holds the promise of greatly shrinking the exploitable attack surface of the enterprise, increasing the impact of the security team and dramatically increasing cyber-resilience.

Balbix BreachControl uses deep learning and advanced AI algorithms to enable you to:

Understand your attack surface Balbix BreachControl continuously observes your extended enterprise network inside-out and outside-in, to discover the attack surface and analyze the hundreds of millions (or more) of data points that impact your risk.

Get an accurate read on your risk Balbix BreachControl 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 heatmaps and Google-like natural-language search. You can ask questions like “where will attacks start” or “what is the risk to customer data”, get a relevant, highly visual answer within milliseconds, and then drill-down into the details.

Obtain prioritized action items with prescriptive fixes

BreachControl 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.

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

