



TAG Cyber •  
**Security Annual**  
2ND QUARTER 2021

**MARKET OUTLOOK &  
INDUSTRY INSIGHTS**

AN INTERVIEW WITH GAURAV BANGA,  
FOUNDER AND CEO, BALBIX

---

EXCERPTED FROM THE FULL REPORT



## AN INTERVIEW WITH GAURAV BANGA, FOUNDER AND CEO, BALBIX

# ARE YOU BLIND AND EXPOSED TO TOO MUCH CYBER RISK?

The enterprise attack surface is already massive and expanding continuously, introducing new risks and threat vectors which enterprise security teams must be aware of and prepared to mitigate. Between weakness in infrastructure, applications, endpoints, IoT, the supply chain, and more, it's hard for security professionals to quantify their company's cyber risk. However, more and more, executives and boards of directors are demanding insight into how their cyber security program is faring and how they can avoid breaches.

Unfortunately, analyzing and improving (i.e., decreasing) cyber risk is no longer human-scale manageable. Millions of continuously changing signals need to be analyzed, correlated, and prioritized for investigation and mitigation.

The key to decreasing cyber risk, says Gaurav Banga, Founder and CEO at Balbix, is automating the pieces of cyber security posture management controlled by just the right amount of human supervision. We spoke with Dr. Banga about continuous security posture assessments, contextualization, automated mitigation workflows, and what it means to calculate and reduce digital risk in a modern business environment.

**TAG Cyber:** *With all the tools and technologies we have today, why is quantifying the attack surface per company still so complicated from a technological point of view?*

**BALBIX:** Let's consider the size of attack surface of a typical enterprise. You might be trying to protect tens (maybe hundreds) of thousands of assets that belong to your organization. Each asset can be compromised in hundreds of ways.

To compute the breach risk of each asset, you need to consider 5 things: asset vulnerabilities, whether these vulnerabilities are being exploited in the wild, the level of exposure of the asset based on how it is used, the presence of any security controls, and the asset's business criticality.


Then there are at least 3 ways in which a compromised asset is impacted: confidentiality, availability, and integrity.

Multiplying these factors to get a back-of-envelope estimate:  $15000 \times 400 \times 5 \times 3$  gives us 90 million factors that need to be continuously observed and incorporated into the enterprise risk calculation. This is not something you can do easily.

Since adversaries tend to target the weakest link, you do need to worry about the complete picture. Any factors you leave out in the calculation above mean you are blind and potentially exposed at the corresponding part of your attack surface.

Reality is even harsher. Most enterprises do not have an accurate picture of their asset inventory. They do not have a full picture of the different types of vulnerabilities and threats, nor do they know the efficacy of their security controls or which assets are most important.

**Multiplying these factors to get a back-of-envelope estimate: 15000 x 400 x 5 x 3 gives us 90 million factors that need to be continuously observed and incorporated into the enterprise risk calculation.**



***TAG Cyber: Why isn't a holistic vulnerability management program, with vulnerability scanning, pen testing, business impact analysis, and incorporating CVEs, for instance, good enough?***

**BALBIX:** Vulnerability assessment is a good start to understanding risk. However, traditional vulnerability management programs miss big chunks of asset inventory. They don't cover many non-CVE risk items such as password reuse, misconfigurations, user behavior, and more. Vulnerability tools also don't understand the compensating effect of deployed security controls. Simply mapping vulnerability metrics to business risk doesn't work because it's missing many factors.

There are many other problems with the way traditional vulnerability management programs are run. Often, there is only episodic assessment when periodic scans are run, which means the picture at any one time is probably a stale snapshot of the past. Organizations don't calculate their mean-time-to-patch (MTTP), which means they don't really know the fraction of time they spend exposed. Business impact analysis is often performed using subjective metrics such as "high," "medium," or "low" rather than in currency terms (e.g., Dollars, Euros, etc.).

Therefore, CISOs and security teams need to do a lot of manual work to gather information from multiple reports and different tools to calculate their overall cyber risk. Many organizations don't even try.

***TAG Cyber: What are the questions your customers—CISOs, specifically—want answered about cyber risk posture?***

**BALBIX:** CISOs have three requirements about cyber security posture:

1. The Big Picture: A unified, up-to-date, comprehensive view of their security posture with accurate risk calculations that incorporate cyber security context and business context.
2. An Operational View: Dashboards, planning tools, workflows, notifications, reports, and more that are integrated with various security and IT tools. The operational view of cyber risk posture helps security teams prioritize projects while enabling the maximum automation and gamification of risk mitigation activities.
3. A Board Level View: An executive view of the big picture, suitable for demonstrating the overall state of the cyber security program to senior executives and board members in business risk terms, while still being firmly tied to the actual on-network conditions.

***TAG Cyber: How does Balbix BreachControl™ work?***

**BALBIX:** In a nutshell, Balbix is about maximum automation of everything needed for cyber risk identification, prioritization, mitigation, and visibility.

Balbix starts by gathering all relevant cyber security and IT data from deployed IT and cyber security tools and directly from the network and endpoints. Note that this telemetry incorporates

data about servers, desktops/laptops, network equipment, smartphone/tablets, IoTs, applications, users; managed or unmanaged; on-prem, mobile, or cloud-based.

This data is constantly deduped, collated, and analyzed to implement automatic asset inventory, and continuously assessed for risk across all assets and 100s of attack vectors. No scans are needed. As new assets are deployed (or old ones repurposed or retired) and as new vulnerabilities become known, Balbix automatically identifies them and recalculates risk, accounting for security and business information. We use proprietary machine learning algorithms to make these complex tasks tractable.

After evaluation, prioritized sets of vulnerabilities are automatically dispatched to the risk owners for supervised and automatic mitigation. Balbix takes into account any exceptions that may have previously been specified. For example, you may have chosen to temporarily accept risk from a CVE because the asset is due to be retired soon. Balbix also lets CISOs specify and manage the risk ownership hierarchy in a systematic fashion. Risk owners have access to all the information, tools, and integrations for automatic as well as supervised risk mitigation.

The cycle is data-driven and highly visual. Each stakeholder has access to contextual dashboards that enable them to do their part in cyber risk reduction.

The role of AI is key in gathering and crunching data. What we do, essentially, is mimic the capabilities of your best cyber security and risk experts, at scale. Unlike human experts, AI models are very good at calculation in 100-dimensional space and can run 24x7 without tiring.

Another key capability we bring is gamification. Forward-leaning CISOs have been trying to do this for many years and Balbix provides a platform to publish risk leaderboards and owners.

***TAG Cyber: How does Balbix manage the “invisible” threat?***

**BALBIX:** By automating asset inventory, Balbix attempts to minimize one component of the “unknown” by accurately identifying things security teams are responsible for protecting.

A second factor of the “unknown” is adversary innovation. We address this by continuously updating models of attack vectors and sequences that we consider in our risk calculations.

The last factor of “unknown” is the human element—human actors will periodically make mistakes and behave in irrational, even malicious ways. This axiom is incorporated into our models and calculations.



