



Decoding Cyber Risk

A framework for understanding
and quantifying cyber risk

What is cyber risk?

Innovations in technology power economic growth and our digital way of life, but at the same time they may have risks, like opening new doors for cyber-criminals. Ransomware, data breaches and other novel cyber-attacks dominate news headlines, and have prompted senior business leaders to ask difficult questions such as “what is our expected financial loss from cyber-attacks?”, “are our cybersecurity investments adequate?” and “what do we need to do differently to reduce our cyber risk?”

To answer such questions, CISOs need to have a rigorous process to analyze their attack surface and quantify cyber risk in monetary units. It starts with defining cyber risk.

Cyber risk includes any financial loss due to disruption in operations, loss of confidential information or damage to the reputation of an organization resulting from the failure of its digital systems. Cyber risk typically stems from:

- Deliberate and unauthorized breaches of security to gain access to data
- Unintentional or accidental breaches of security

Key questions for stakeholders:

- What cyber breach scenarios would be catastrophic?
- What data/systems can we do business without and for how long?
- What information absolutely cannot fall into the wrong hands?
- What could cause personal harm to employees, customers, partners, visitors?

WHERE DOES CYBER RISK COME FROM?

Cyber risk has increased as digital transformation, globalization, and distributed workforces, have led to employees, customer and partners being linked through a web that extends beyond the traditional borders of your corporate network. Risk is also present due to the multitude of devices and applications in your network. These assets include internal servers, managed endpoints, infrastructure components such as routers, switches, DNS servers, and domain controllers, unmanaged devices, corporate and personal cloud applications, connected IoT devices and apps, 3rd party software and portals, and much more.

This risk can manifest itself in many forms. Enterprise assets are susceptible to a wide range of attack methods, from simple ones like exploiting weak or default passwords, unpatched software and misconfigurations; to more sophisticated ones such as phishing and social engineering. At any given time, there are literally hundreds of viable attack vectors for attackers to choose from.

By plotting *enterprise assets against attack vectors*, we can visualize the enterprise attack surface. Every point on this attack surface represents a potential area of compromise, and therefore risk. This attack surface is massive and expands as your organization grows. The attack surface for a typical mid-sized enterprise with 5,000 employees has over 50 million data points. For larger enterprises, this number explodes to 100 billion or more.

Risk is the third dimension of the attack surface, and is represented below in Figure 1 in order of magnitude as grey, green, yellow, orange or red.

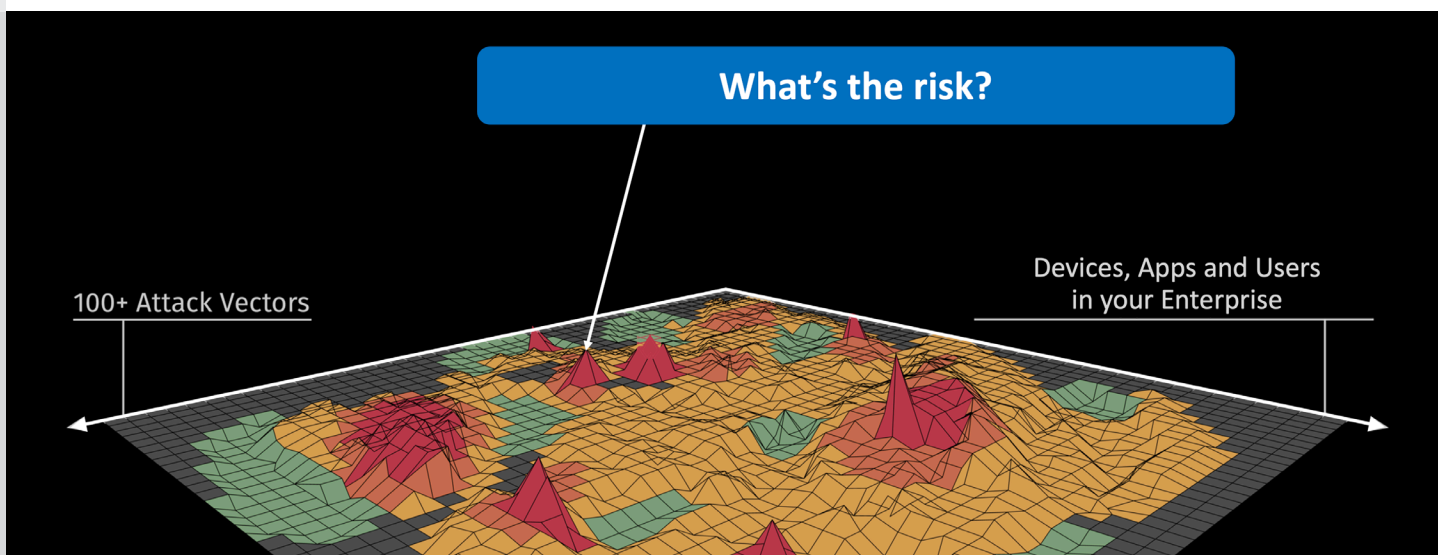


Figure 1: A representation of an enterprise attack surface

THE IMPORTANCE OF QUANTIFYING CYBER RISK

The ability to quantify cyber risk accurately is fundamental to making the right decisions about your cybersecurity posture. There is no such thing as zero risk, and the leaders of each organization must decide for themselves if their organization's residual cyber risk is acceptable. It is critical that cyber risk is quantified in monetary terms for a CFO, CEO and board to appreciate the amount of risk in business terms. A risk score that is denominated in color codes (like Figure 2 above), as high/medium/low or on a scale of 1-10 is not very useful for decision making. For example, executives and board members will not be able to appreciate that a score of 7 out of 10 corresponds to a high likelihood of a data breach with a \$25M price tag.

A calculation of cyber risk should:

- Be in units of money
- Incorporate the effect of vulnerabilities, exposure, threats, security controls and business criticality
- Cover the vast majority of the attack surface
- Be continuous, automatic and in near real-time
- Be available for inspection. One must be able to drill down from a risk value to the asset attributes, specific user behaviors or metrics driving the risk
- Allow for human input and overrides
- Be accompanied by a prioritized set of mitigating actions and an estimate of the reduction to cyber risk if they are carried out

CHALLENGES IN QUANTIFYING CYBER RISK

A mature infosec program typically involves investing in dozens of cybersecurity tools including vulnerability management, endpoint detection and response (EDR), next-gen IDS/IPS, a SIEM and detection and containment playbooks; and likely involves doing regular pen-testing, perhaps augmenting this with a Breach Attack Simulation (BAS) tool and an outside-in risk scoring tool. But, for most organizations, calculating cyber risk remains elusive.

Here are three brutal truths about quantifying cyber risk by using traditional security tools and processes:

1 **Data ≠ Visibility.**

Your cybersecurity tools may be generating terabytes or petabytes of data. However, mountains of data do not result in better cybersecurity visibility. It is difficult and time-consuming to sift through this data to find indicators of risk as the required data is spread out across security, IT and business tools. Cybersecurity context tends to reside mostly in specialized cybersecurity tools. IT context is spread across multiple IT tools such as AD, CMDB and ticketing systems, while business context tends to be spread across a 3rd set of databases and spreadsheets.

2 **Can't Calculate Risk.**

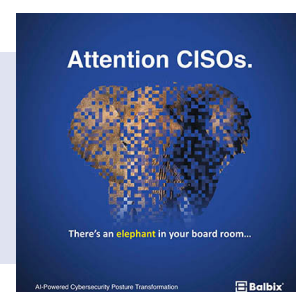
It is also very difficult to unify this data into a common risk schema. Tools have different formats and semantics for the same attributes of assets or users, or worse, they surface contradictory information. Different stakeholders also speak using different terminology, and it is nearly impossible to reconcile them to a commonly understood risk metric.

3 **Partial Remediation.**

A third issue is that security issues and risk items cannot be quickly identified, prioritized and remediated. In most organizations, the mean time to mitigate security issues is weeks or months, and during this time the organization is open to compromise by attackers. Moreover, new vulnerabilities and security issues emerge at a very rapid rate.

If you have a developing infosec program, and have deployed the tools mentioned above, you may find this eBook useful:

[How to Gain 100x Better Visibility into your Cybersecurity Posture](#)



QUANTIFYING CYBER RISK

To obtain a quantifiable measure of risk, risk can be defined as the probability of a loss event occurring in a given unit of time (Likelihood) multiplied by the expected magnitude of loss resulting from that loss event (Impact). Cyber risk is the expected loss resulting from a cyberattack or data breach.

The equation for risk is as follows:

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

In the risk equation, the units of *Impact* are monetary *units*, e.g., dollars, euros, yen, pounds etc. *Likelihood* is a probability, typically expressed as a percentage value. Multiplying these two factors together gives us the units of risk as *monetary value of the expected loss event occurring in a defined time period*.



Calculating the Likelihood of a Breach

Breach likelihood is defined as the probability of a loss event occurring in a given unit of time. Let's look at what factors influence the breach likelihood for an asset.

Breach likelihood is a probabilistic function of 4 factors: **Vulnerabilities**, **Threats**, **Exposures**, and **Security Controls**. Let's examine each of these factors in turn.

#1. VULNERABILITIES

A vulnerability, according to the traditional definition, is anything that exposes you and puts you at risk. In cybersecurity, the word vulnerability is closely associated with unpatched software flaws (also referred to as [CVEs](#)). However, weak or default passwords, reused passwords, misconfigurations, encryption issues, and the risky online behavior of employees are all vulnerabilities from a cyber risk standpoint.

Unfortunately, most enterprise vulnerability management programs focus only on unpatched software flaws and don't monitor their attack surface for other risk items. To accurately calculate breach likelihood and risk, you must factor in vulnerabilities across a broad range of attack vectors and breach methods including those described below:








Vulnerabilities are not just CVEs. Any breach methods that put your enterprise at risk are dangerous.



Do You Know?

What's your risk from weak or shared passwords, encryption issues, online behavior of your admins and other vulnerabilities?

Most common breach methods

		
Phishing, Web & Ransomware	Compromised Credentials	Weak Passwords
		
Trust Relationships & Propagation	Poor Encryption	Unpatched Vulnerabilities
		
Misconfigurations	Malicious Insiders	Zero Day & Unknown Methods

#2. THREATS

Attackers generally like to use techniques that are reliable and easy to use. It is important to map real and emerging threats such as those currently fashionable (or possible) for the adversary to specific assets. Vulnerabilities with active threats increase risk, while the ones that are very hard to exploit and don't have active threats can be de-prioritized.

Sometimes attackers will use specific techniques to attack organizations of a particular type. As part of the risk calculation, it is important to understand which ones are important to your organization.

#3. EXPOSURE

This factor incorporates items such as how an asset is placed on the enterprise network, e.g., outside the firewall vs. in an isolated subnet, its frequency of use, as well as type of use. For example, if default web browser is Google Chrome, should a vulnerability in Internet Explorer, even with publicly available exploit code as a threat, increased your risk?



Do You Know?

What vulnerabilities are being exploited in the wild?

#4. SECURITY CONTROLS

Infosec programs typically include several security tools as protective controls to mitigate risk from a wide range of known and unknown vulnerabilities. This investment into security controls like EDR, firewalls and anti-phishing systems influences breach likelihood. For example, the presence of a browser isolation solution can lower the risk of drive-by phishing considerably.



Do You Know?


Which of your deployed security controls are effective in reducing risk from your open vulnerabilities?

Calculating Breach Impact

Breach impact is the magnitude of harm expected to result from the consequences of unauthorized disclosure, modification, destruction, or loss of information. In simple terms, impact is correlated to the business criticality of an asset. Criminals are interested in customer, employee, and financial data, intellectual property, contract terms and pricing, strategic planning data, and third- and fourth-party vendor data. They also know they can extract a ransom if they can control the availability of the underlying systems.

To accurately calculate impact of a breach, you first need to understand which assets in your network would be potential targets for cyber criminals and then quantify their importance to your business in monetary units. Breach impact can be determined by examining each asset's type, role(s), access, users and other attributes.

For example, your breach impact is significantly higher for core servers containing sensitive data than for personal smartphones sequestered on your guest network. An attack on your company's source code repositories is likely to have a greater impact than the guest sign-in kiosks in your building lobby. While assessing business criticality of an asset, you need to consider both inherent (e.g., asset category, business unit) and contextual properties of the asset (e.g., roles, applications, user privilege, and interaction with other assets).

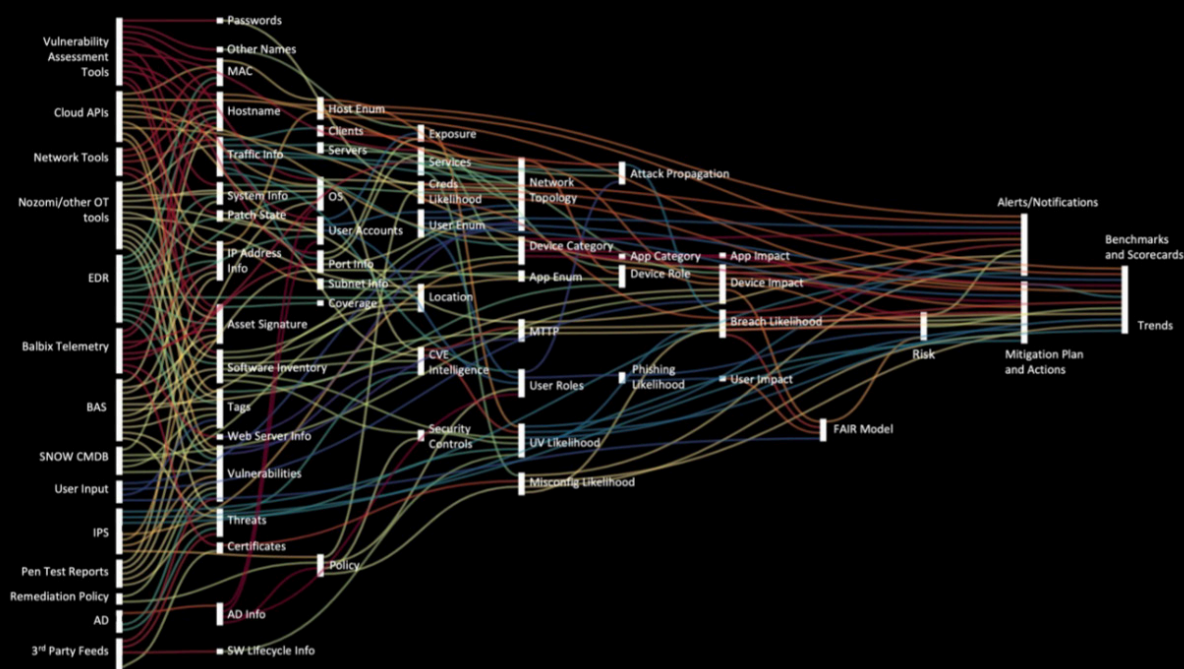
 **Do You Know?**

What is the importance or "business value" of each asset?

To understand your organization's cyber risk profile and breach impact, you need to determine what information would be valuable to outsiders or cause significant disruption if unavailable or if the data it holds is corrupted.

How Balbix Can Help

Balbix enables organizations to produce a single, comprehensive view of their cyber risk, by ingesting, unifying and analyzing data from a broad set of IT, cybersecurity and business tools. The Balbix platform uses specialized machine learning and automation to quantify both the likelihood and the impact of a potential breach, and remove complex and error-prone tasks, and quantify your enterprise's cyber risk in dollars (or other currencies).



This picture shows how typical inputs from various IT, cybersecurity, and business data sources are processed and analyzed within the Balbix brain. The outputs such as risk metrics, mitigation plan and actions, alerts/notifications, benchmarks, scorecards and trends, are available to users via online dashboards, customizable based on role.

Each interior node represents an ensemble of specialized ML models that has been purpose-built to solve a specific problem in the overall risk calculation.

For example, the host enumeration (Host Enum) node performs deduplication of assets across all data stream signals that are fed into the Balbix brain and provides this information to all nodes in the system. There are nearly a hundred ML models like Host Enum in the Balbix brain.



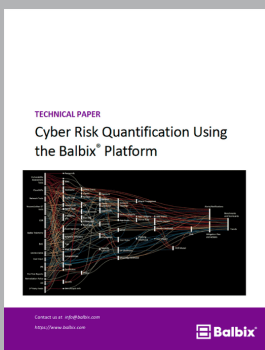
Figure 2: The Balbix executive dashboard showing breach likelihood and breach impact and the resulting risk to the organization

More details about Balbix’s cyber risk quantification capabilities can be found [here](#).

ABOUT THE BALBIX PLATFORM

Balbix automatically analyzes the enterprise attack surface using specialized AI to provide a 100x more accurate view of breach risk. The Balbix platform enables a broad set of use cases that help you automate your cybersecurity posture, reduce cyber risk and improve resilience.

Our customers have seen fantastic outcomes from Balbix: an accurate and unified asset inventory, better risk prioritization, 98% reduction in mean time to mitigate risk issues, and a 10x improvement in efficiency of everyday infosec team activities. Everyone is on the same page because all dashboards and widgets speak to risk in monetary terms. Our customer CFOs actually understand and appreciate what is happening in the infosec program!



Read this technical
whitepaper to learn more
about Balbix's Cyber Risk
Quantification solution