



eBook

Decoding Cyber Risk

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

What is cyber risk?

Innovations in technology power new strategic initiatives but at the same time, they open new doors to cyber-criminals. Attacks by hackers dominate everyday headlines prompting senior business leaders to routinely ask tough questions like “what are our top cyber risks?” and “are our cybersecurity investments in the right areas?”

To answer such questions, CISOs need to have a rigorous process to measure and analyze cyber risk. Before we get into that, let’s start with defining risk.

Risk is defined as the probability of a loss event (likelihood) multiplied by the magnitude of loss resulting from that loss event (impact). Cyber risk is the probability of exposure or potential loss resulting from a cyberattack or data breach. Per NIST, cyber risk is a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

Mathematically, cyber risk can be denoted by multiplying likelihood of breach and its impact:

$$\text{risk} = \text{likelihood} \times \text{impact}$$

Key questions for stakeholders:

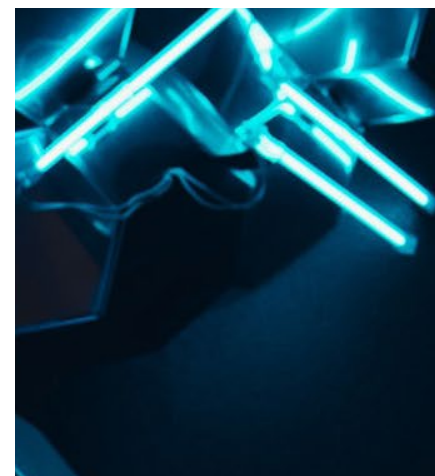
- What losses would be catastrophic?
- What data/systems can we do business without and for how long?
- What information absolutely cannot fall into the wrong hands or be made public?
- What could cause personal harm to employees, customers, partners, visitors?

Where does risk come from?

With digital transformation, increase in globalization, and distributed workforce, there is an interconnected web of employees, customer, and third-party vendors linked to the enterprise network. There are also a multitude of applications and devices also connected to your network. These devices and apps 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, 3rd party vendors, and much more. Together, these are your full complement of enterprise IT assets.

Your assets are susceptible to a wide number of attack methods, from simple ones like exploiting weak or default passwords, to more sophisticated methods like phishing, social engineering, known unpatched software issues and zero-day vulnerabilities. There are hundreds of such attack vectors at the adversary's disposal.

If you plot all of the enterprise assets against the various methods of attack that might be used by the hackers, you have a massive attack surface for your enterprise. Every point on this attack surface represents a potential area of compromise, and therefore, risk

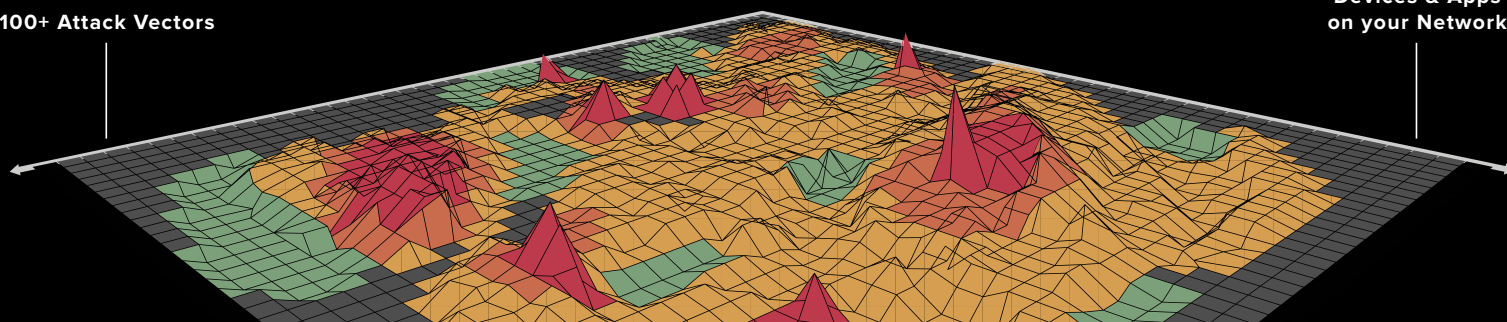


Cyber risk is defined as any risk of financial loss, disruption or damage to the reputation of an organization resulting from the failure of its information technology systems. Typically, cyber risk could materialize from:

- Deliberate and unauthorized breaches of security to gain access to data
- Unintentional or accidental breaches of security
- Operational IT risks due to factors such as poor system integrity

100+ Attack Vectors

Devices & Apps
on your Network



The attack surface expands as your organization grows, as you adopt new technologies, and as the bad guys come up with new ways to compromise your organization. For a mid-sized enterprise with 1,000 employees, there are over 10 million time-varying signals that must be analyzed on an ongoing basis to predict breach risk. For larger enterprises, this number explodes to 100 billion or more signals.

Likelihood of breach

One intuitive notion that all security practitioners agree with—given enough effort, anything can be breached.

The likelihood of a breach, as defined by NIST, is a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability. An intuitive notion that all security practitioners agree with is that given enough effort, anything can be breached. Graphically, the Breach Likelihood vs Effort concept is depicted below (Figure 1).

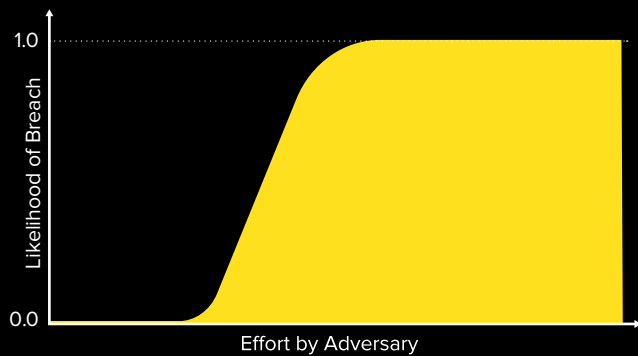


Figure 1: Breach Likelihood vs Effort

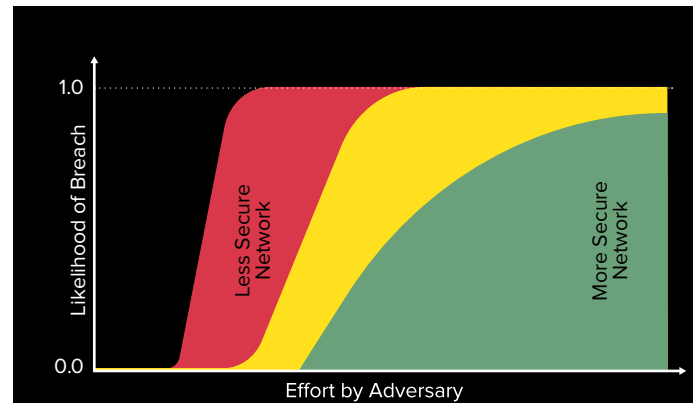


Figure 2: Breach Likelihood vs Effort for organizations of different security maturity levels

Every enterprise has a Breach Likelihood vs Effort curve like the one shown in Figure 1. However, the placement of the knee of the curve on the x-axis, and the slope of the rise from 0 to 1 may be different. Intuitively, you might think that a security-mature company like a Fortune 500 bank might have the knee of the curve well towards the right of the axis. A smaller company, with a less mature cybersecurity program, might have the knee shifted more towards the left (Figure 2). This is largely true. But there is also a natural entropy in play that tends to move larger, more complex networks closer to the left. All else equal, the larger attack surface makes it easier to break into a network with 10,000 moving parts than it is to break into a network with 10 moving parts.

[Download the eBook](#)



Consider this. Would this curve remain the same for your network at all times?

The short answer is—no. As you make changes to your network, the curve changes. The deployment of a new security control might push the curve significantly to the right, decreasing the slope. The discovery of a new vulnerability in your network which is being exploited in the wild will move the curve to the left and perhaps make it steeper, until the vulnerability is patched. Given that your network is dynamic with new devices and users, new applications, new configurations and vulnerabilities, upgrades and patches happening continuously, this Likelihood vs Effort curve changes on a daily basis.

The dynamic nature of the enterprise network necessitates continuous, real-time visibility into your enterprise asset inventory. Maintaining an accurate inventory allows measurement, the first step towards understanding your overall breach risk.

¹ While these are multi-dimensional variables, for the sake of illustration these have been mapped to 2 dimensions.

Risk calculation challenges

Legacy vulnerability & patching tools use primitive risk metrics. Likelihood and Impact are usually given values of between 1 and 3 or 1 and 5 resulting in a grid. An example of a 5 x 5 grid can be seen below:

Risk Rating = Likelihood x Severity

S e v e r i t y	Catastrophic	5	5	10	15	20	25
	Significant	4	4	8	12	16	20
	Moderate	3	3	6	9	12	15
	Low	2	2	4	6	8	10
	Negligible	1	1	2	3	4	5
			1	2	3	4	5
			Improbable	Remote	Occasional	Probable	Frequent
			Likelihood				

Catastrophic	■	STOP
Unacceptable	■	URGENT ACTION
Undesirable	■	ACTION
Acceptable	■	MONITOR
Desirable	■	NO ACTION

The Common Vulnerability Scoring System (CVSS) provides a numerical (0-10) representation of the severity of an information security vulnerability.

Using CVSS scoring to prioritize risk is inadequate

Originally, CVSS scoring was conceived as a way to streamline information exchange about vulnerabilities between the industry stakeholders. By assigning each vulnerability a severity score from 1 to 10, CVSS attempts to establish an objective measure of the severity of any given vulnerability. It takes into account criteria such as access vector, attack complexity, authentication requirements and impact, among others.

However, using CVSS scores alone to prioritize vulnerabilities is not how they were originally intended to be used. Traditional tools that scan for vulnerabilities and prioritize remediation efforts by CVSS scores are leaving your organization open to breach risk. Relying on CVSS scores for vulnerability management is likely to cause security teams to squander resources on patch cycles that focus on low-impact, low-probability issues or prioritize vulnerabilities that don't actually pose the biggest threat to the environment.

4 factors influencing likelihood of breach

Likelihood of breach is a function of 4 factors: vulnerabilities, threats, exposures, and mitigating controls. Let's examine each in further detail.

$$\text{risk} = \text{likelihood} \times \text{impact}$$

likelihood = f(vulnerabilities, exposure, threats, mitigating controls)

#1. Threats

Opportunistic attackers do not care about whom they attack and with new threats emerging on a daily basis, it is key to understand which ones are important to your organization. Attackers only utilize threats that they know how to exploit, and many exploits have never been realized beyond their theoretical potential. Since most attackers are only skilled enough to use pre-existing tools, attack techniques come in and out of fashion as tools are developed, and as security teams learn to thwart those attacks reliably. Mapping real and emerging threats - what is currently fashionable (or possible) for the adversary—to specific assets and then observing and prioritizing them is critical.



Do You Know?

What weaknesses are being exploited in the wild?

It is also important to keep in mind that not every threat realizes a risk. Threats require vulnerabilities in the target system to become successful attacks. For example, a malformed network packet is only harmful if the software processing the data packet enters an undefined state which allows the attacker to take over control. Such vulnerabilities emerge from common mistakes during coding, which are hard to fully avoid in software development. Likewise, the social engineering attempt is only successful if the victim is tricked into sharing credentials with unauthorized parties.

An exploit is when attackers take advantage of software bugs or vulnerabilities, giving them unauthorized access to a system and its data. Commonly exploited software includes operating systems, Internet browsers, Adobe applications, and Microsoft Office applications.

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

#2. Vulnerabilities

A vulnerability, according to the traditional dictionary definition, is anything that exposes you and puts you at risk. Typically, the word vulnerability is closely associated with unpatched software, but bad password hygiene—using weak or default passwords, reusing passwords, and not storing passwords correctly—is also a vulnerability. And so are misconfigurations, encryption issues, and risky online behavior of employees. However, a large percentage of organizations running vulnerability management programs utilizing traditional scanners only monitor for unpatched software flaws or CVEs (publicly known infosec vulnerabilities and exposures in publicly released software packages) and don't monitor their attack surface for other risk items. To accurately calculate risk, you must factor in vulnerabilities across a range of attack vectors.












Do You Know?

What's your risk from weak or shared passwords, malware, phishing, encryption issues, online behavior of your admins and more?

It is also important to keep in mind that not every threat realizes a risk. Threats require vulnerabilities in the target system to become successful attacks. For example, a malformed network packet is only harmful if the software processing the data packet enters an undefined state which allows the attacker to take over control. Such vulnerabilities emerge from common mistakes during coding, which are hard to fully avoid in software development. Likewise, the social engineering attempt is only successful if the victim is tricked into sharing credentials with unauthorized parties.

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

#3. Exposure

Exposure due to asset usage is a critical, multi-dimensional factor that influences likelihood of breach. This encompasses items such as duration for which the asset has been present on the network, availability and frequency of use, as well as type of use. In addition to these, it is also important to take into account usage at a different levels of granularity, including individual software and applications, the user profile on the asset (e.g. a Virtual Desktop Interface (VDI) can be used by different users over time), as well as the rate and entropy of credentials used to access a service on the asset. For example, if a piece of software hasn't been opened in 6 months, should a vulnerability in that software be your highest infosec priority?

Do You Know?



Based on how an asset is used, what is its exposure to a particular vulnerability?

Assets that are highly used are likely to be more vulnerable to a breach.

#4. Mitigating Controls

Security organizations typically apply several compensating controls—both products and policies—to mitigate risk from a wide range of vulnerabilities. This investment into security controls like firewalls, anti-phishing systems, and EDR influences the likelihood of breach. For example, the presence of a micro-virtualized browsing solution can lower the risk of drive-by phishing considerably.

Similarly, an organization that is effective and timely in its patching behavior decreases its exposure to breach via unpatched vulnerabilities. On the other hand, an organization that rarely patches its critical systems increases its exposure to a breach as unpatched vulnerabilities arise and fail to be remediated.

Do You Know?



Are there any current security controls in use that are reducing the risk?

Calculating impact

Impact of a breach, according to NIST, is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure, modification, destruction, or loss of information. In simple terms, impact represents the business criticality of a given information system asset.

To complete our calculation of risk, impact must be calculated for every device, app and user located within your network. This impact is determined by examining each asset's type, roles, access and many other attributes. Your breach impact is significantly higher for core servers containing sensitive data than for personal smartphones sequestered on your guest network.

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 enumerate their importance to your business. Criminals are interested in your customer, employee, and financial data, intellectual property, contract terms and pricing, strategic planning data, and your third- and fourth-party vendor data.

impact = g(business criticality)

risk = likelihood x impact

likelihood = f(vulnerabilities, exposure, threats, mitigating controls)

Assessing business criticality

The interaction between threats, vulnerabilities, and controls determines the success of attacks. Considering the business criticality of assets as an individual risk factor governing impact is important because more important assets should have an outsized percentage of information security resources assigned to their protection. Your company's source code repositories should be emphasized much more 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 (roles, applications, user privilege, and interaction with other assets).



Do You Know?

What is the importance or “business value” of each asset?

The value and criticality of affected assets influences the potential impact of an incident

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 corrupt.

Measuring and analyzing cyber risk

To accurately measure risk, you need to first understand and calculate your likelihood of breach (which is a function of threats, vulnerabilities, exposures, mitigations afforded by existing security controls) and secondly, determine the potential impact of a breach, a function of business criticality of assets. That may sound simple theoretically, but in reality, this translates to several crucial steps.

#1 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 and infrastructure, BYODs, IoTs, cloud, third party 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.)

#2 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.

#3 Prioritize actions that offer greatest breach risk reduction

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 prioritized, not just as 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”.

GET

continuous, real-time visibility into inventory, vulnerabilities, threats, and mitigations.

MAKE

your security practice preventative and proactive instead of reactive.

ALIGN

your cybersecurity posture with cyber risk.

How Balbix can help

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



Understand your attack surface

Balbix 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 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,” 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 BreachControl™

Balbix BreachControl platform uses specialized AI algorithms to discover and analyze the enterprise attack surface to give a 100x more accurate view of breach risk.

Balbix enables a broad set of vulnerability and risk management use cases that help to transform your enterprise cybersecurity posture, reducing cyber-risk by 95% or more, while making your security team 10x more efficient.

Click below to explore use cases

100x Cybersecurity Posture Visibility



Risk-Based Vulnerability Management



Cyber-Risk Reporting for Board of Directors



Automatic Asset Inventory



Gamification of Cybersecurity Posture Transformation



Visibility and Security of IoTs, OT and Cloud Assets

