CYE

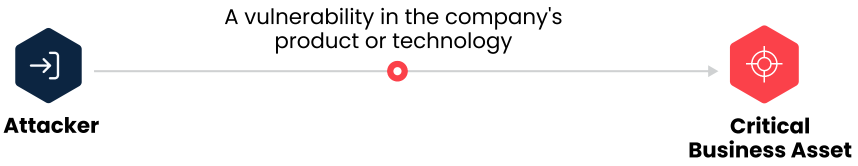
How Hyver Uses AI

Hyver, CYE's optimized cyber risk quantification platform, uses advanced technology to generate business insights that empower companies to make effective cybersecurity decisions. Here's how.

Edge Probability Model

In Hyver, an edge is represented as a line drawn from one position to another, which typically represents a finding—a vulnerability that is detected. Using AI and machine learning, Hyver calculates the likelihood that this vulnerability can be exploited in that particular organization.

For example, a vulnerability such as a weak password policy can be the edge between an attacker and an asset. The asset can range from a client database to control over a computer that manages the organization's website or critical infrastructure.



A vulnerability in the company's product or technology

Attacker

Critical Business Asset

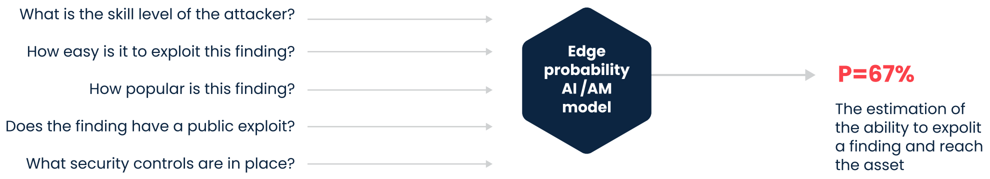
Using AI, the edge model:

- Examines how many times our team of ethical hackers was able to exploit a finding
- Detects if the finding has been subverted or blocked by security controls in the organization
- Considers other factors, such as attacker skill level, the ease of exploitation, the popularity of the finding, and security controls in place

Data sources used:

- National Vulnerability Database
- ExploitDB
- CVSS
- Over a decade of CYE's assessments

How Hyver calculates the probability of an attacker exploiting a finding:



What is the skill level of the attacker?

How easy is it to exploit this finding?

How popular is this finding?

Does the finding have a public exploit?

What security controls are in place?

Edge probability AI /AM model

P=67%

The estimation of the ability to exploit a finding and reach the asset

Likelihood of Breach

To determine the likelihood of a breach, Hyver creates a customized attack graph depicting security gaps that lead to critical business assets.

For example, in a potential attack scenario, the origin might be an exposed testing environment or weak password policy. Using AI, Hyver's model considers all the findings, routes, and threat sources to calculate the likelihood of reaching the organization's critical assets.

Cost of Breach Model

Hyver leverages over 220,000 datapoints, incorporating specific organizational parameters such as geolocation, industry sector, and size, to anticipate potential damages and calculate the expected cost of breach (COB).

Data sources include:

- Advisen breach database
- Ponemon Institute
- Cyber insurers' claim data
- CYE's incident response team (over a decade of assessments)

Using business information and details about attacks on organizations, Hyver examines the total costs involved in the event of a breach. It then calculates COB by multiplying the average COB (based on factors such as sector or geolocation) by the company's security posture.

Industry COB according to sector, geolocation, size, revenue, etc. **X** Increase or decrease in COB according to the security posture of the company **=** **Expected COB**

Want to learn more about how Hyver can help you manage cyber risk? **Contact us.**

About CYE

CYE's optimized cyber risk quantification platform and expert guidance transform the way organizations manage cybersecurity. Using AI, machine learning, and extensive data, CYE visualizes attack routes, quantifies cyber risk, provides evidence-based mitigation plans, improves communication between CISOs and executives, and matures organizational cybersecurity posture. In doing so, CYE provides clear and relevant insights that empower companies to make effective cybersecurity decisions. The company serves organizations in multiple industries globally. Founded in 2012, with headquarters in Israel and operations around the world, CYE is funded by EQT and 83North. Visit us at cyesec.com.