CYE
Real Cybersecurity

THE GUIDE TO CHOOSING A CYBER RISK QUANTIFICATION STRATEGY

How CYE helps you understand the true cost of cyber incidents and remediation so you can optimize security budgets and reduce risk of breaches.

> By 2023, 30% of a CISO's effectiveness will be directly measured on the ability to create value for the business.
>
> Gartner

OVERVIEW

Companies in every industry and of every size face the challenge of managing cyber risk. As threats have grown more sophisticated and widespread, organizational cybersecurity budgets have increased as well. Therefore, it's not surprising that in recent years, business executives have expected security leaders to not only define their organization's cybersecurity policy, but to also justify costs. Execs understandably want reassurance that cybersecurity solutions and resources are truly warranted and that they indeed are worth the investment.

Businesses undoubtedly benefit by working closely with security teams. By communicating with decision-makers and being aligned with business needs, CISOs can ultimately help security be perceived as a business enabler, rather than a blocker. But how can this be accomplished?

Enter cyber risk quantification, which aims to put a dollar figure on cyber risk. It considers the potential financial and business ramifications of possible cyberattack scenarios, thus allowing decision-makers to understand the impact of threats and prioritize remediation efforts. In addition, it allows CISOs to communicate the value of their work to execs.

In theory, it sounds like a great strategy, but not all cyber risk quantification solutions are the same.

CURRENT SOLUTIONS FALL SHORT

Cyber risk quantification begins with a risk assessment, and many solutions measure cyber risk by providing a risk score or level. Much like a credit rating, this is a number that provides an overview of the state of an organization's security posture. Yet there are a few issues with this:

The reality is that only a small portion of vulnerabilities are leveraged by an attacker. How can you identify which ones need to be addressed?

They lack risk context. The cyber risk score might reveal a small or large number of cyber gaps, which would result in a good or poor rating. However, sometimes malicious actors can plot attack routes to important business assets by exploiting just a few vulnerabilities. Likewise, a significant number of cyber gaps may seem highly problematic on the surface, but they may not present any serious threat to your most important business assets. The reality is that only a small portion of vulnerabilities are leveraged by an attacker; how can you identify which ones need to be addressed?

They lack financial context. In addition to understanding the risk to business-critical assets, organizations must take into account the dollar value of what a breach to each asset might be. This financial context, which is typically lacking with risk scores, helps security teams make better decisions about which cyber gaps must be addressed first. For example, a low threat to a $1 billion asset would take priority over a high threat to a $1 million asset.

They lack breadth. Risk scores or levels are based on what has been assessed, which does not necessarily include the entire organization. A truly comprehensive assessment would need to check cyber risk in multiple environments, including on-prem, cloud, perimeter, and OT.

They lack coherence. Because so many environments must be assessed, organizations often must rely on numerous solutions to help manage cyber risk. This can be arduous and ineffective, because it's difficult for people to try to interpret reports from multiple vendors to determine which risks are most likely to cause the most damage and should be addressed.

Because such cyber risk assessments are inadequate, any subsequent cyber risk quantification based on them is inherently flawed. The result is wasted time, effort, and money prioritizing risk and remediating vulnerabilities that do not significantly impact the business, while the most threatening cyber gaps may not be addressed effectively.

Meanwhile, board members demand visibility into cyber risks that organizations face, as well as the cost of fixing them. How can you focus on the vulnerabilities that truly pose a threat to your organization?

INTRODUCING **CYE**

CYE considers multiple factors when calculating an organization's cyber risk. They include:

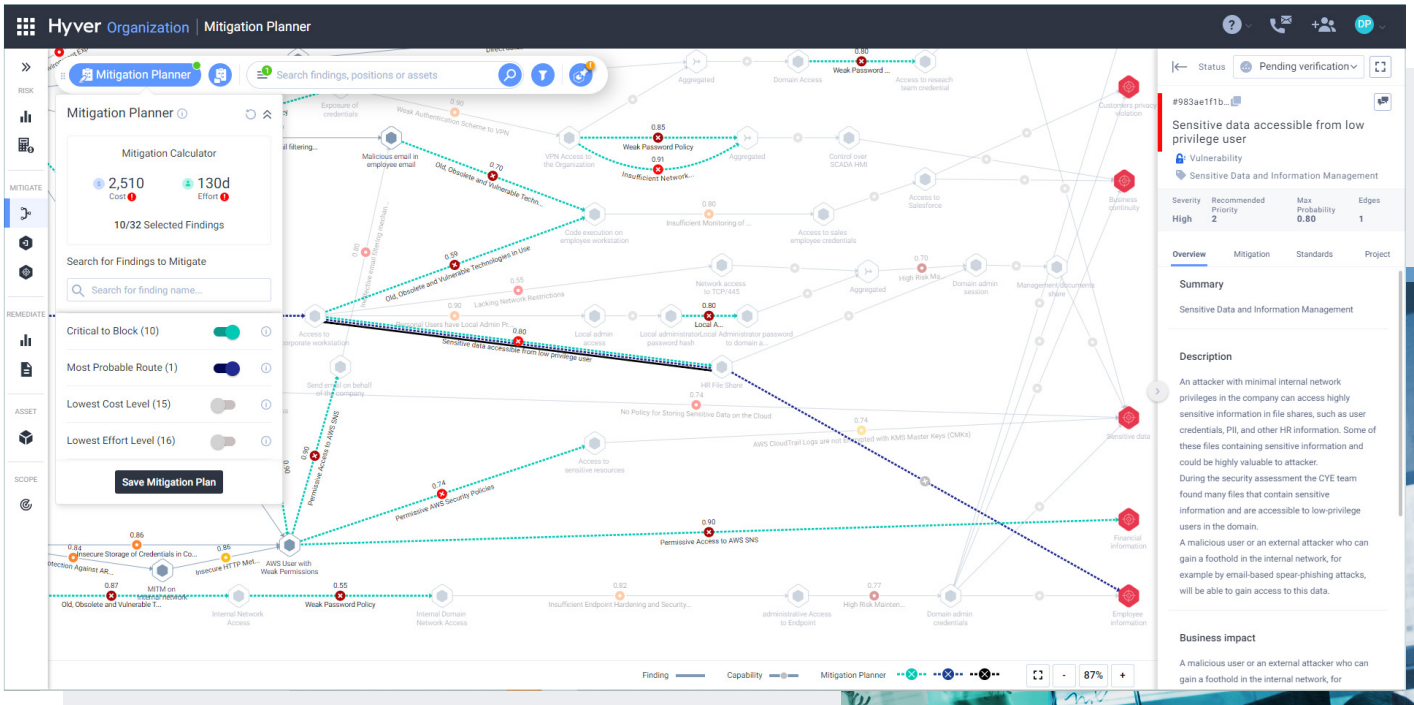
The type of attacker. This can be a cybercriminal, an insider, or someone from the supply chain.

The business assets at risk. This can be customer information, employee information, intellectual property, or business continuity.

The environments. CYE calculates attack scenarios through multiple environments, including the cloud, the internet perimeter, applications, and more.

The true threat of vulnerabilities. For example, vulnerabilities that are not connected to essential business assets do not share the same risk level as vulnerabilities with a direct route to critical or sensitive data. Similarly, vulnerabilities that require permissions would be more difficult to exploit.

Using this data, CYE provides realistic views of possible attack routes. Using cyber risk quantification, CYE then determines which vulnerabilities should be fixed and their costs. CYE also provides the cost of a breach if the vulnerabilities are not fixed.



THE BENEFITS OF CYBER RISK QUANTIFICATION WITH **CYE**

Some immediate benefits of using CYE for cyber risk quantification become evident. With CYE, you can:

Understand your organization's true cyber risk

CYE bases its assessment on which assets are specifically at risk, including customer information, employee information, or business continuity. Using red team activity and technology, CYE plots multiple possible attack routes and determines the key cyber gaps that must be closed to avert such attacks.

Know how technical risks translate into business risks

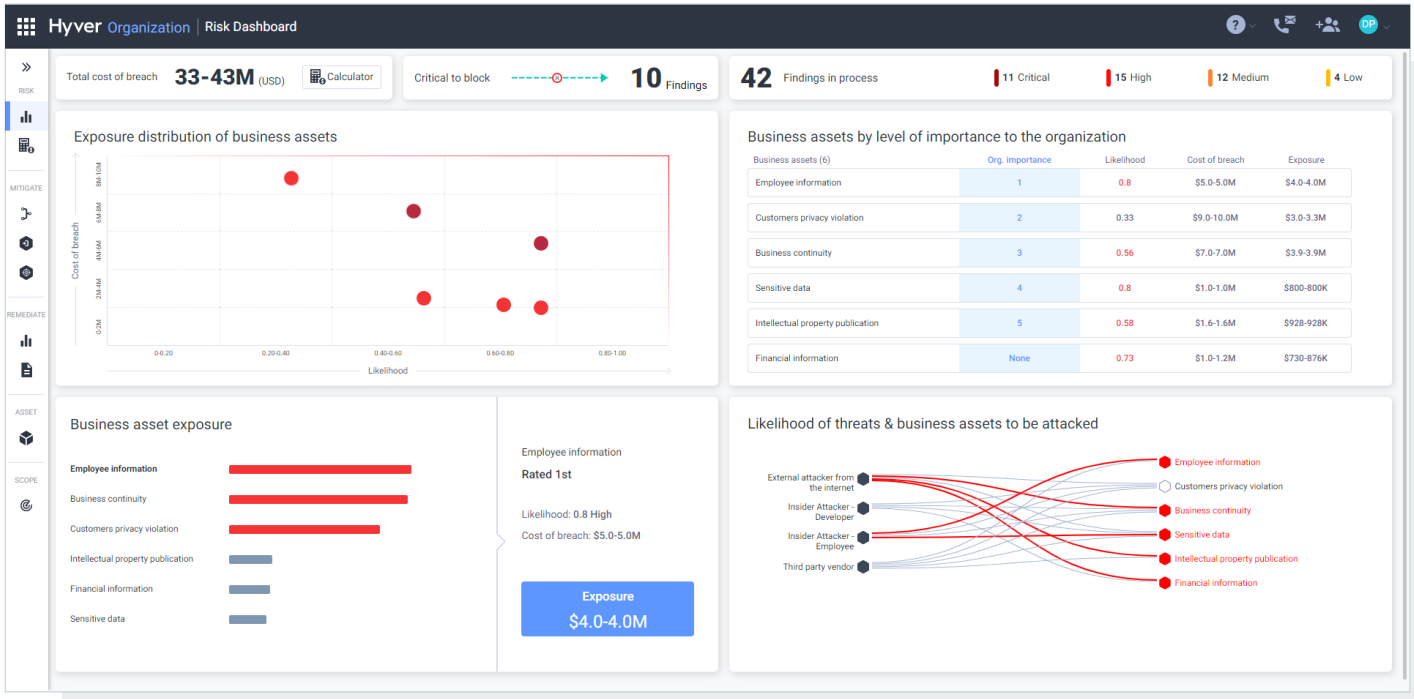
CYE correlates asset value, the severity of findings, and threat actor activity. Using cyber risk quantification, security teams can track, report, benchmark, and optimize their security effectiveness. In doing so, CYE provides realistic cybersecurity investments that consider both the cost of a possible cyber incident and the cost of remediation. This helps your business save time and money.

Receive a customized mitigation plan

CYE provides a mitigation plan that prioritizes actions according to specific business considerations and goals such as financial impact, security maturity, and loss exposure. This way, you get a clear view of your investment and expected ROI, so you can focus on what matters the most for your company.

Avoid an expensive data breach

According to IBM, the average cost of a data breach in 2021 was $4.24 million, up from $3.86 million in 2020. With larger companies, that figure was as high as $5.52 million. Clearly, organizations have a vested interest in reducing cyber risk. CYE's strategy, which effectively shuts down attack routes, has been proven to be extremely effective in protecting businesses against cyberattacks.



To sum up, companies using CYE:

Make better risk investment decisions by understanding the cost of threats and remediation

Benefit from prioritization of mitigation planning according to financial and business impact

Can communicate cyber risk in business terms, allowing management to make better decisions about reducing risk

Would you like to learn more about how you can realistically quantify your organization's cyber risk using CYE?

Schedule a Demo

ABOUT **CYE**

CYE's cybersecurity optimization platform enables businesses to assess, quantify, and mitigate cyber risk so they can make better security decisions and invest in effective remediation. CYE combines this with dedicated professional guidance and advice provided by established cybersecurity experts. The company serves Fortune 500 and mid-market companies in multiple industries around the world. With headquarters in Israel and offices in New York and London, CYE is funded by EQT Private Equity and 83North. Visit us at cyesec.com.