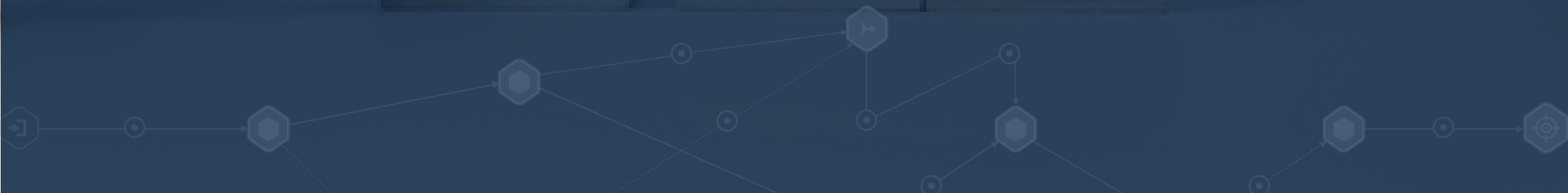




Cyber Risk Quantification: Building an Effective Strategy

Building an evidence-based CRQ strategy for budget optimization and risk reduction.





Overview

"By 2025, 50% of cybersecurity leaders will have tried, unsuccessfully, to use cyber risk quantification to drive enterprise decision making."

Gartner

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 (CRQ)**, which is the process of calculating an organization's risk exposure and the potential budgetary impact of that risk in business-relevant terms. Cyber risk quantification 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 CRQ Solutions Fall Short

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?

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

- **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 the right financial context.** In addition to understanding the risk to business-critical assets, organizations must consider 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. Instead of customizing the data, many organizations use external reports that not necessarily aligned with their unique business information.
- **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?

Features of Effective CRQ Solutions

A truly effective cyber risk quantification model understands and parses the data, deriving risk information that has meaning and is easily communicated to the C-suite and the board. It takes into account constantly evolving and newly emerging threats, providing continuous visibility into the cybersecurity landscape.

Once the required information (assets and value, likely threats and probabilities, potential damage, and vulnerability of critical assets) is plugged into the model, the immediate output is a metric indicating organizational risk. At this point, optimal cyber risk quantification models will also incorporate data to assess the attack likelihood for each business asset, calculating the specific probability of each business asset being breached and the associated cost.

Highly effective cyber risk quantification models will map out possible attack routes to each critical asset along with their probabilities. Using AI and machine learning, the model will consider all relevant data: This includes multiple factors such as type of attacker, business assets at risk, the environment and current threat landscape, and the impact of vulnerabilities.

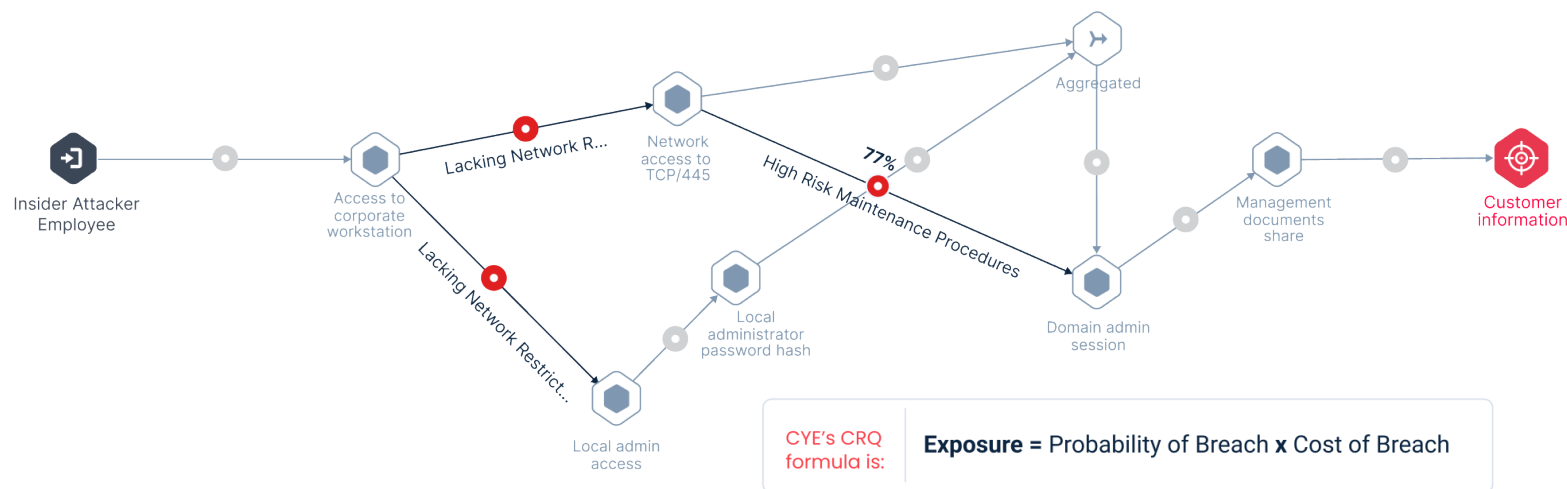
The model should provide realistic views of all possible attack routes. This level of visibility helps the security team reduce overall exposure, prioritize actions, and take proactive measures to reduce the likelihood of becoming a cyberattack victim. Perhaps most importantly, the model should prioritize mitigation efforts based on the extent to which they actually reduce risk. This makes it possible for CISOs and security professionals to stop relying on ineffective severity-based (or in many cases gut-based) approaches for prioritizing mitigation, which are detached from risk modeling.

How Effective CRQ Helps CISOs

As businesses adapt to digital-first and cloud-first strategies, the role of the Chief Information Security Officer (CISO) within modern enterprises is undergoing significant transformation. Today's CISO not only collaborates directly with C-level executives and the board of directors to provide insights into cybersecurity threats and mitigation strategies, but also contributes to informed strategic business decisions.

As boards of directors become more attuned to cybersecurity matters, they increasingly expect CISOs to regularly report on the organization's cybersecurity posture. According to Gartner, it is projected that "By 2025, 40% of boards of directors will establish a dedicated cybersecurity committee led by a qualified board member, a substantial increase from the current less than 10%."

Cyber risk quantification, done right, can help today's CISOs translate cyber risk into business risk: It presents security risk in monetary terms that management can understand.

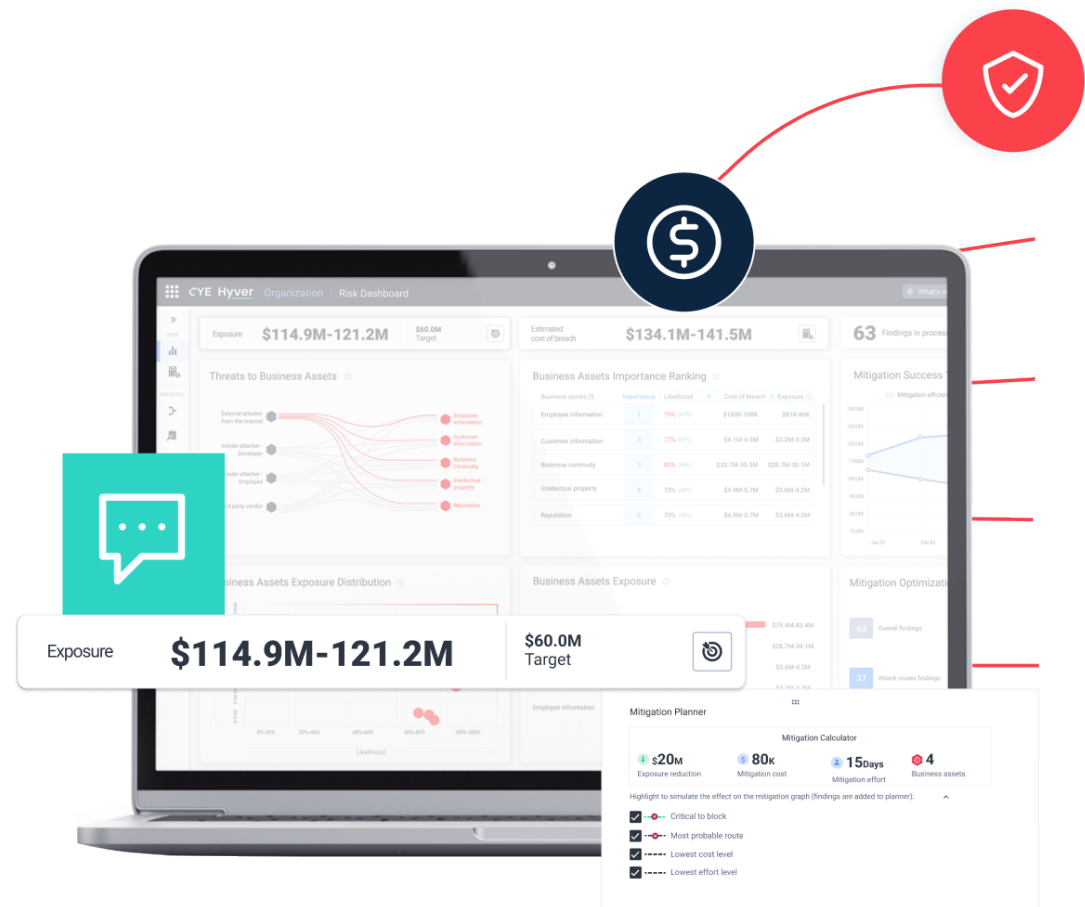


Introducing Hyver

CYE's optimized cyber risk quantification platform, Hyver, 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, Hyver visualizes probable attack routes. Using advanced algorithms and data models for cyber risk quantification, it then determines which vulnerabilities should be remediated and their costs. Hyver also calculates the cost of a breach if the vulnerabilities are not remediated.



The Benefits of Cyber Risk Quantification with Hyver

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

Understand your organization's true cyber risk

Hyver bases its assessment on which assets are truly at risk, including customer information, employee information, or business continuity. Using AI, machine learning, and innovative technology, Hyver 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

Hyver 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, Hyver focuses on 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

Hyver's mitigation planner 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 2023 was \$4.45 million—the highest figure ever. Clearly, organizations have a

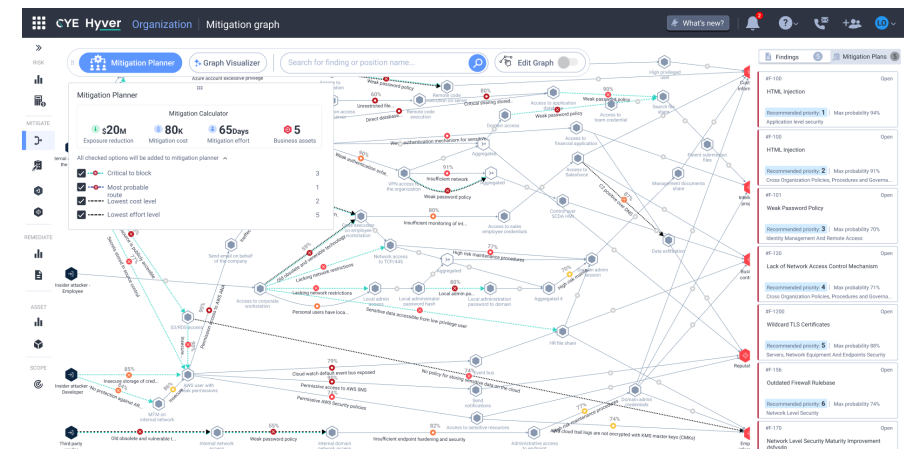
strong interest in reducing cyber risk. Hyver's strategy, which effectively shuts down attack routes, has been proven to be extremely effective in protecting businesses against cyberattacks.

Communicate effectively with stakeholders

Because Hyver focuses on how cyber risk can impact the business, it speaks the language that executive teams can understand. Instead of presenting endless vulnerabilities with technical jargon, security leaders can present a comprehensive cybersecurity plan that ultimately benefits the organization.

Bolster your cybersecurity maturity

Hyver also quantifies organizational cybersecurity maturity, allowing you to set targets, benchmark against your industry, and track your progress over time. It relies on CYE's objective and continuous data, as well as your security team's input.





To sum up, companies using Hyver:

- Gain complete visibility of probable attack routes leading to critical business assets.
- Make better risk investment decisions by understanding the cost of threats and remediation through a dynamic risk calculation.
- Streamline and prioritize mitigation planning based on real evidence and build an efficient business continuity plan.
- Greatly reduce the likelihood and potential impact of a cyberattack.
- Effectively communicate with executive teams and stakeholders about cyber risk.
- Benchmark with similar companies to find out where they stand.

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

Contact us to schedule a demo.

About CYE

CYE's optimized cyber risk quantification platform and expert guidance transform the way organizations manage cybersecurity. Using AI, machine learning, and innovative technology, CYE visualizes attack routes, quantifies, mitigates, and communicates cyber risk, 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 Private Equity and 83North. Visit us at cyesec.com.