CYE

Technical Paper

How CYE Performs Cyber Risk Quantification and Mitigation Optimization

Paper Goal & Outline

This paper describes CYE's methodology for quantifying organizational cyber risk and prioritizing remediation based on optimal risk reduction, as it is implemented in Hyver, CYE's exposure management platform.

In our terminology, **we use the term exposure interchangeably with risk**, to address **the expectancy of loss** due to a cyber event.

The general flow of the method is as follows:

1. CYE creates a comprehensive and validated (real-world) view of cybersecurity vulnerabilities and findings that lead potential attackers to the organization's Business Critical Assets (BCAs) from all possible attack surfaces. This is performed by using findings from organizational risk assessments, penetration testing assessments, and security tools, assisted by our automation framework and AI engines.

2. CYE generates a graph representation of the findings and attack routes. This representation describes the assessment process and details all operations and assets leveraged by CYE to gain access to BCAs, from zero-privileges external locations.

3. The graph is enriched with statistical information, labeling each finding with probability for exploitation. This data is then used to compute the probability of breach for each of the BCAs, which is then aggregated to organizational probability of breach; i.e., **organizational cyber exposure**.

4. The graph and statistical framework are used as inputs for CYE's mitigation optimization algorithm. The algorithm prioritizes the findings according to maximized exposure reduction. This means that **findings that reduce exposure the most will be prioritized above others**. The algorithm further produces a set of critical-to-block findings, which upon mitigation, allow the organization to cut off attackers from BCAs and greatly reduce exposure.

For brevity and focus, this paper will detail steps 2 and 3 of our methodology. We will only address key aspects of steps 1 and 4 for completeness.

Organizational Assessment

As mentioned, we will not outline this part of CYE's method for cyber exposure calculation. We will only point out key features which are critical for the accuracy of our exposure calculation:

1. The assessment approaches the organization from all possible (permitted) attack vectors. This includes all internet facing assets, on-prem access, vendors, etc.
2. The assessment relies on no pre-supplied credentials or authentication. This is key for staying true to real-world attack scenarios.
3. The assessment evaluates all aspects of the organization cybersecurity posture, from purely technical findings to organizational policies and employee behavior.
4. The assessment reports only true positives – verified vulnerabilities and security gaps - and specifically those that could be leveraged towards compromising a BCA.

Next, we describe CYE's mitigation graph, and how it illustrates the attack and list of findings.

Mitigation Graph

The Mitigation Graph outlines all the possible attack routes that may be exploited by an attacker towards gaining access and control of the organization's BCA.

In the Mitigation Graph:

- Nodes are organizational assets that may be compromised by an attacker
- Edges are findings and vulnerabilities exploited by attackers to gain access to assets
- Edges are weighted by the probability of exploitation for the finding they represent
- Sink nodes (nodes with only incoming edges) are the organization's Business Critical Assets (BCAs), representing the goal for an attacker e.g., sensitive data, intellectual property etc.
- Source nodes (nodes with only outgoing edges) are entry positions e.g., internet facing services or vendor API

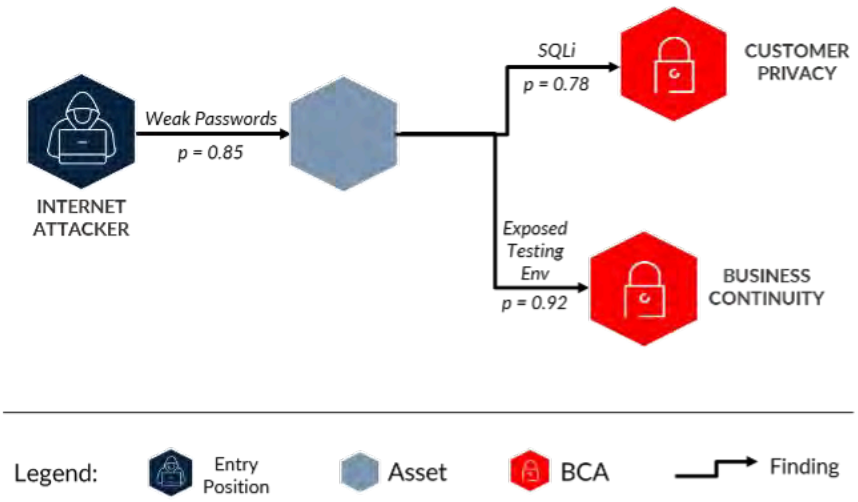


Figure 1 – Simple mitigation graph

Computing Organizational Cyber Exposure to BCAs

Organizational cyber exposure is an aggregation of the exposure to the organization's BCAs. This stems from CYE's definition of organizational cyber exposure:

$$Exposure(ORG) \triangleq$$

the expectancy of loss to the organization's ***business critical assets***

$$= \sum_{\substack{Business \\ Critical \\ Assets}} Likelihood\ of\ Breach(BCA) \times Cost\ of\ Breach(BCA)$$

BCA Exposure

BCA exposure is based on the exposure each of the possible attack routes pose to the asset. We illustrate this with the following example of an attack route:

Attack flow:

An external attacker

- Initiated the attack from the internet
- Reused an employee's passwords which were obtained from a previous data leak
- Gained access to a user account
- Leveraged high privileges of the user
- Reached an SQL server
- Gained access to private customer info

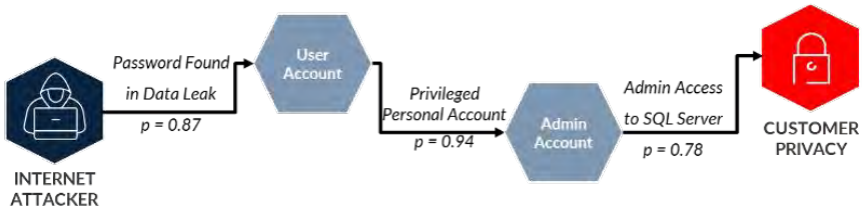


Figure 2 - Attack route example

Route Probability Calculation

The overall probability of the route is a product of the probability of the findings. In our example the probability will be:

$$Risk(Customer\ Privacy) =$$

$$p(Password\ Found\ is\ Data\ Leak) \times p(Privileged\ Personal\ Account) \times p(Admin\ Access\ to\ SQL\ Server) =$$

$$0.87 \times 0.94 \times 0.78 =$$

$$\mathbf{0.67}$$

Multiple Routes & Recurring Findings

We note that attack scenarios to BCAs are almost never as simple as the case above. In many cases, a BCA will have multiple routes leading to it, with the same finding recurring (in different use case scenarios) over the routes, as is depicted in the following example.

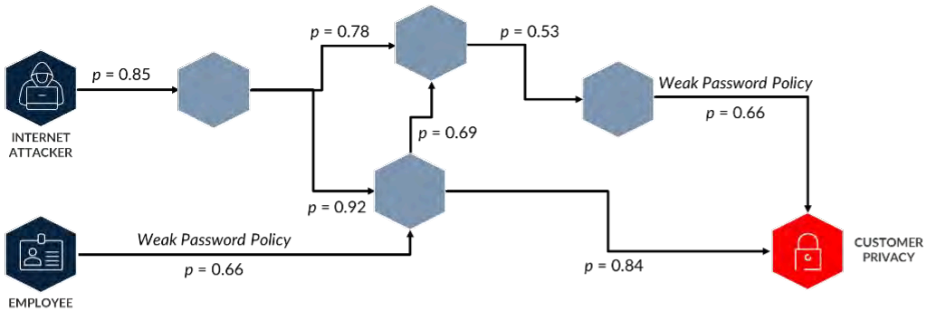


Figure 3 - Multiple routes with recurring finding leading to BCA

Hyver's sophisticated statistical algorithm accurately calculates the exposure to the BCA, i.e., $Risk(Customer\ Privacy) = P(Route\ 1 \cup Route\ 2)$.

Assigning Cost of Breach to BCA for Organizational Exposure

We revisit our exposure formula:

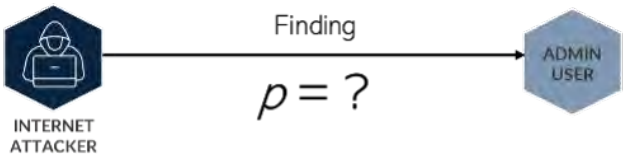
$$Exposure \triangleq \sum_{\substack{Business \\ Critical \\ Assets}} Likelihood\ of\ Breach(BCA) \times Cost\ of\ Breach(BCA)$$

After describing how the likelihood of breaching each BCA is calculated, we only require **assigning cost of breach** to each to the BCAs to finally determine the overall exposure.

Cost of breach estimation is performed by **CYE's Cost of Breach Model**. See the "CYE Cost of Breach Model" data sheet for more details.

Edge Exploitation Probabilities

A key pillar of our methodology is the specific finding probability. We must be able to accurately quantify the probability of a finding, which is akin to assessing the overall probability of it being exploited, to truly assess exposure.

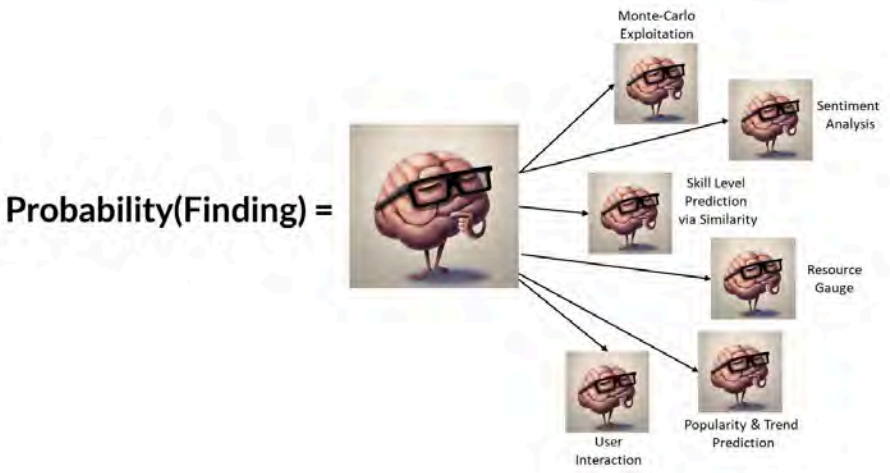


Probability Estimation Factors and Models

Our model for computing finding probability relies on various internal (in-house CYE knowledge, threat analysis, and tools) and external (global cybersecurity trends, community knowledge, exploits publication, etc.) factors. To illustrate our approach, here are some of these factors:

Factor Name	Description
Organizational Maturity	The maturity level at which the organization operates, in categories related to the finding.
Finding Complexity	The amount of effort and general level of know-how required for successfully exploiting the finding.
User Interaction	The type of user interaction, whether it be passive (i.e., requires an operation that is routinely performed) or active (i.e., actively engaging the user).
Exploitability	The availability and readiness of external tools and exploits required for successful exploitation.
Finding Popularity	The level of usage (i.e., a trend indicating the finding is on the rise).

Each probability factor is approximated using our data models. Some of them are:



Example: Popularity and Trend Prediction Model

The popularity prediction model allows us to identify trending findings and vulnerabilities and adjust their probability of exploitation accordingly.

To do so, we rely on data we collect from our internal sources (assessment data and internal feeds from our cybersecurity researchers) and external data we collect from sources such as:

- CVE databases
- Social media chatter
- News outlets
- Community forums

The data is fed into our AI platform, which leverages language models to identify references to findings, and tags the sentiment of that reference. The flow of information allows our model to identify an increase or decrease in the popularity of a finding and adjust the probability in all existing and future mitigation graphs.

Mitigation Prioritization

The organizational cyber exposure CYE determines, beyond being an informative and accurate assessment of the organization's cybersecurity posture, is crucial in allowing the organization to make informed and correct decisions in its mitigation efforts. This allows organizations to cut through the noise and focus on the real issues that put them at risk.

Hyver, using BCA exposure and weighting, employs advanced graph algorithms to optimally prioritize findings.

Conclusion

In this paper, we described CYE's methodology for cyber risk quantification and mitigation optimization using the Hyver platform and its mitigation graph. This methodology is based on a real-world comprehensive view of the organization's cybersecurity posture and a deep statistical framework and algorithms built to calculate exposure and optimally mitigate it. Our technique is tried and tested, as it was developed over years of assessments for hundreds of customers.

Want to learn more about how CYE can help you with cyber risk quantification and mitigation optimization? Contact us.

About CYE

CYE's exposure management platform, Hyver, transforms the way security teams protect their organizations. With CRQ at its core, the platform reveals enterprises' exposure in financial terms, visualizes the most exploitable attack routes to critical business assets, and creates mitigation plans tailored to each business. CYE's customized reporting enables the sharing of vital board-level metrics and validating exposure reduction over time. In addition, CYE improves cybersecurity maturity by mapping weaknesses and defining targets based on industry frameworks. Founded in 2012 in Israel with operations around the world, CYE has served hundreds of organizations across industries globally. Visit us at cyesec.com.

1000 North West Street, Suite 1410, Wilmington DE 19801, United States
1 Ballards Lane, London N3 1LQ, UK | Abba Eban 10, Herzliya 4615200, Israel