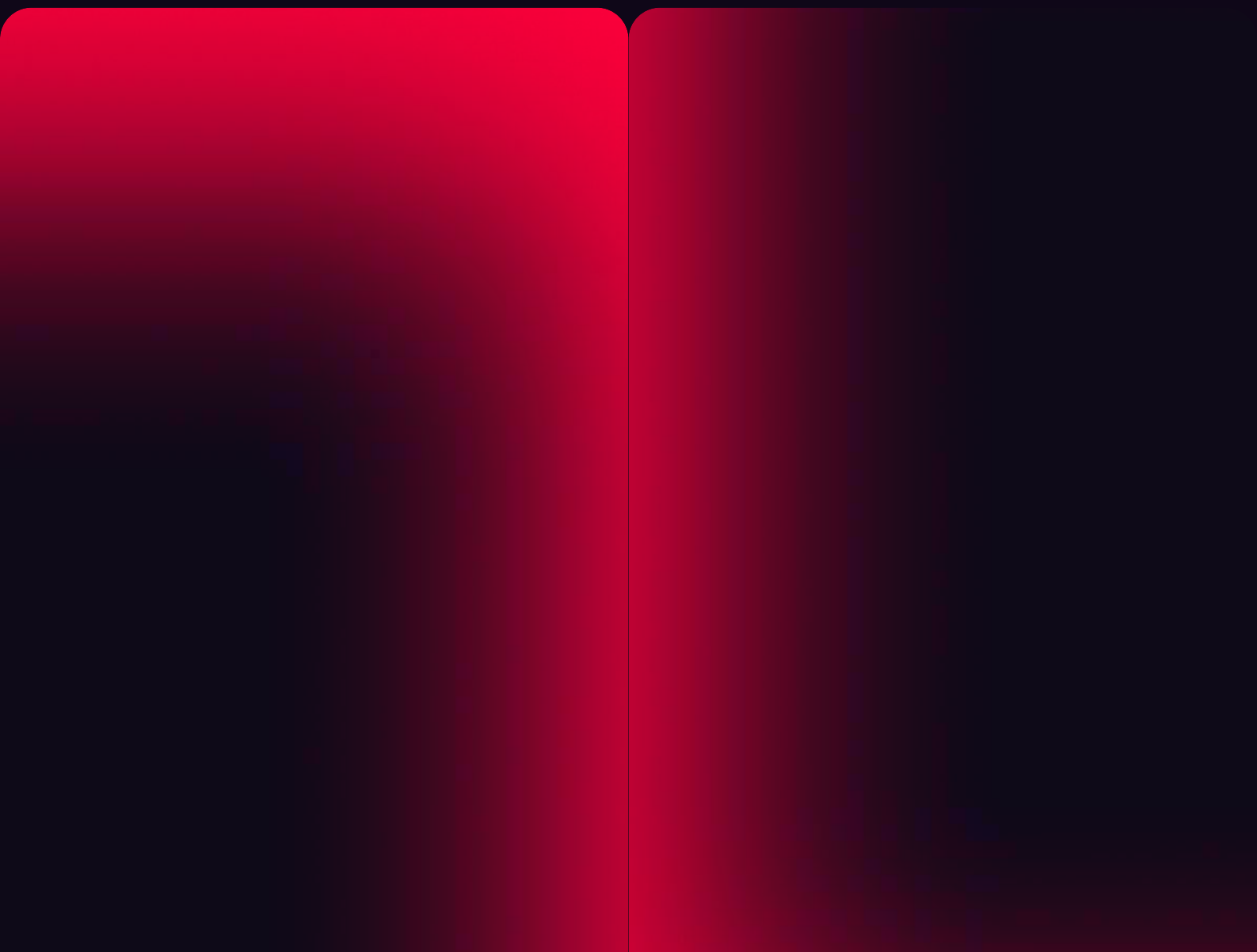
HADRIAN

GUIDE

Beyond ROI: A guide to Value of Loss Avoidance



A better metric for offensive cybersecurity

You are constantly watching the Return on Investment (ROI) in your tooling. But, when it comes to offensive cybersecurity, the best way to prove value is to compare it to the cost of a data breach. ROI, while still valuable in certain contexts, doesn't tell the full story. This document will show you how to use a new equation to determine the value of your offensive cybersecurity tools.

Cost of data breaches

THE AVERAGE TOTAL COST OF A BREACH. UP 10% OVER PREVIOUS YEARS AND CONTINUES TO CLIMB.

4.88 MILLION USD

AVERAGE YEAR-OVER-YEAR GROWTH IN COST OF DATA BREACH.

10% AND RISING

COST SAVINGS FROM EXTENSIVE USE OF AI IN PREVENTION.

2.2 MILLION USD

Source: IBM Cost of a Data Breach Report, 2024

The value of loss avoidance

While the substantial costs associated with a data breach are tangible, the value of proactive prevention can appear abstract, complicating the presentation of a clear financial case for security investments. Traditional Return on Investment (ROI) metrics, though effective in many business domains, fall short in cybersecurity, struggling to accurately quantify the impact of prevented incidents. Here, **the Value of Loss Avoidance (VLA) presents a superior solution by directly quantifying the investment in mitigating exposures against the potential financial losses from cyber incidents**, thus providing a clear method to demonstrate how security expenditures actively protect businesses from significant breaches.

The VLA is a simple complementary metric to ROI where you exchange the net profit with losses avoided.

Simple, right? Not so fast.

To achieve a more accurate calculation based on data and not averages or speculation, there is a handy table that can help you determine a more accurate scope of cost.

Likelihood of exploitation scale (LES) ranges

The **Likelihood of Exploitation Scale (LES)** helps assess the probability of a given exposure being successfully exploited. This scale, ranging from 0 to 10, provides a clear framework for understanding the urgency and potential impact of various exposures.

Very high likelihood (10 – 8)

These exposures are almost certain to be targeted by adversaries and are often actively exploited in the wild. This category includes zero-days, publicly disclosed flaws with working exploits, and unauthenticated remote code execution weaknesses frequently used in attacks.

High likelihood (8 – 3)

Exposures in this category are highly susceptible to exploitation. Attackers commonly target remotely accessible flaws, weaknesses in widely deployed technologies, and issues requiring minimal effort to compromise.

Moderate likelihood (3 – 1)

Exposures in this range have a reasonable chance of exploitation but typically depend on additional conditions. Attackers may exploit flaws that require user interaction, specific network positioning, or uncommon configurations to succeed.

Low likelihood (1 – 0.2)

These exposures are unlikely to be exploited without significant effort. Exploitation generally necessitates complex attack chains, specialized knowledge, or privileged access, limiting their appeal to attackers.

Very low likelihood (0.2 – 0)

Exposures in this category are rarely exploited due to strong mitigations, minimal visibility, or niche attack requirements. Attackers typically disregard flaws in isolated systems, legacy environments with strict access controls, or those requiring very specific conditions for compromise.

Calculating mitigated loss based on identified exposures

When estimating mitigated losses, it is crucial to account for the probability of exploitation within the investment timeframe. To precisely calculate the mitigated loss for each exposure severity, we begin by mapping the number of identified exposures alongside a breach impact assumption. This is the estimated financial cost of a breach at that severity level. Next, the LES is used to quantify the probability of successful exploitation for each exposure severity. The LES represents the likelihood of an exposure being exploited within a defined timeframe.

This calculation yields the mitigated loss per exposure. Loss per exposure can be calculated depending on the average cost of the following:

- Data recovery costs
- Legal fees
- Compliance and regulatory fines
- Cost of business disruption
- Forensic investigations
- Increased insurance premiums

This transforms abstract probabilities into quantifiable financial figures. For example, considering a sample set of identified exposures, the calculation would appear as follows:

EXPOSURE RATING	LES	LOSS PER EXPOSURE
Critical	3	$ 146,400
High	1	$ 34,160
Medium	0.5	$ 4,880
Low	0.1	$ 195

Differences per industry

Unfortunately, not all cyberattacks are created equal and there are certain industries that cybercriminals target more than others due to high margins, valuable data, or confidential intellectual property.

Whatever their reasons, certain industries should be prepared to add a multiplier to their total number of exposures to accommodate for the increased pressures these industries face. You can use this table as reference:

INDUSTRY	Exposure Multiplier
MANUFACTURING	x7 total number of exposures
FINANCE	x7 total number of exposures
HEALTHCARE	x5 total number of exposures
GOVERNMENT	x4 total number of exposures
ENERGY	x3 total number of exposures
RETAIL	x2 total number of exposures
OTHER	No multiplier

Calculating the VLA

Keeping in mind that exposures rarely occur in a vacuum and many exposures often occur in concert with other exposures, your costs could start adding up very quickly. In a conservative instance, if you have 3 critical exposures ($146,400 cost per exposure), 5 high exposures ($31,160 cost per exposure), 8 medium exposures ($4,880 cost per exposure) and 12 low exposures ($195 per exposure), you quickly get to a data breach cost of **$636,380**.

Let's return to our Value of Loss Avoidance equation: VLA = Total loss avoided - Cost of tool investment

We will also plug in our assumptions with an average cost of an offensive security tool at $70,000.

The VLA in this estimation totals over half a million dollars. The loss caused by the breach dwarfs the cost of the tool that could have prevented the breach in the first place.

Provide measurable financial savings for your board of directors

The Value of Loss Avoidance (VLA) empowers security teams to effectively justify budget requests by quantifying the potential financial impact of mitigated exposures. This approach demonstrates how strategic investments in security tools proactively prevent costly incidents, translating abstract security exposures into clear financial metrics that resonate directly with executives and board members.

Unlike traditional metrics, such as the number of incidents prevented or the percentage of exposures mitigated, which often fail to convey their financial significance to business leaders, VLA shifts the focus to measurable financial outcomes. This precisely illustrates how cybersecurity investments directly enhance an organization's bottom line.