EPIPHANY

# Redefining Risk:

## Vulnerability vs. Exploitability

31 HUDSON YARDS, 11TH FL NEW YORK, NY 10001 (800) 794-4985 INFO@EPIPHANYSYS.COM WWW.EPIPHANYSYS.COM EPIPHANY

Cybersecurity has been a struggle for organizations since the dawn of the internet, but over the past few years, it has become significantly more challenging. New technologies, digital transformation, and the shift to a remote/hybrid work model have all contributed to expanding the attack surface and making it more complex. At the same time, the line between nation-state attacks and cybercrime has blurred, and threat actors continue to adapt and refine their tactics, techniques, and procedures (TTPs) to make the threat landscape more sophisticated.

Business and cybersecurity success both depend on the same thing—effectively minimizing and managing risk. It is daunting to consider, though, and difficult to even know where to start. There was a record-breaking 28,695 vulnerabilities identified in 2021. **That's an average of more than 550 new vulnerabilities to address every week.**

It is virtually impossible to patch or mitigate every vulnerability and threat, yet vulnerability management is the primary strategy for reducing risk for many cybersecurity programs. The net result is that IT security teams are stressed, overwhelmed, and scrambling to keep up. Poor prioritization consumes precious resources while leaving the business exposed to risks with potential material impact.

Organizations need to stop chasing vulnerabilities and instead focus on exploitability. It's time to adopt an approach of exposure management.



## What Is Risk?

If the goal of cybersecurity is to minimize and manage risk, the first step is to understand what risk is. The Merriam-Webster Dictionary defines risk very broadly as, "Possibility of loss or injury."

The Institute of Risk Management provides a more specific meaning from a cybersecurity perspective. "'Cyber risk' means any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems."

According to EY, "Cyber risk is the risk of financial loss, disruption of activities, impact on the company's image or reputation as a result of malicious and purposefully executed actions in the cyber space. Cyber risks may have an impact on the confidentiality, integrity and availability of information systems and their related data."

31 HUDSON YARDS, 11TH FL NEW YORK, NY 10001 (800) 794-4985 INFO@EPIPHANYSYS.COM WWW.EPIPHANYSYS.COM EPIPHANY

## Vulnerability vs. Exploitability

The term vulnerability implies that there is an identified flaw or weakness that a threat actor might be able to exploit or take advantage of to execute a malicious attack. Based on these definitions, vulnerabilities objectively expose an organization to risk, but it's important to recognize that not all vulnerabilities are created equally. The reality is that not all vulnerabilities are exploitable. More importantly, not all exploitable vulnerabilities are being actively exploited, and not all actively exploited vulnerabilities have the potential for material impact.

With an average of 550 new vulnerabilities every week, it is unrealistic and impractical to try and patch or mitigate all of them. Vulnerabilities are essentially limitless, and even the best vulnerability management strategies will never address them all. Vulnerability management programs generate reports and overwhelming lists of required remediations that IT security teams generally cannot keep up with, which leads to an expanding attack surface and greater exposure to risk.

You can make the vulnerability management approach significantly more manageable if you narrow it down to vulnerabilities that have known exploits—or even further to vulnerabilities that are confirmed to be actively exploited in the wild. CISA (Cybersecurity and Infrastructure Security Agency) maintains the Known Exploited Vulnerabilities Catalog, which currently has just under 800 vulnerabilities listed.

However, even that approach is lacking important context that could result in poor prioritization and inefficient use of resources. Effective exposure management requires that we redefine risk.

## Redefining Risk

An IT security team has limited resources, and an overwhelming volume of vulnerabilities and threats to address, so it's crucial to evaluate and prioritize risk effectively. For effective cybersecurity, though, the definitions cited above fall short. They are valid definitions in the abstract but lack the context necessary to evaluate and prioritize risk in an IT environment.

The NIST (National Institute of Standards and Technology) definition is more accurate for understanding risk for cybersecurity. "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs; and the likelihood of occurrence."

Risk is not a black and white issue, though. Risk is subjective. It is determined by a variety of factors and perspectives that are unique for each organization and environment. Risk is also a moving target. Risk and the measurement of it change over time.

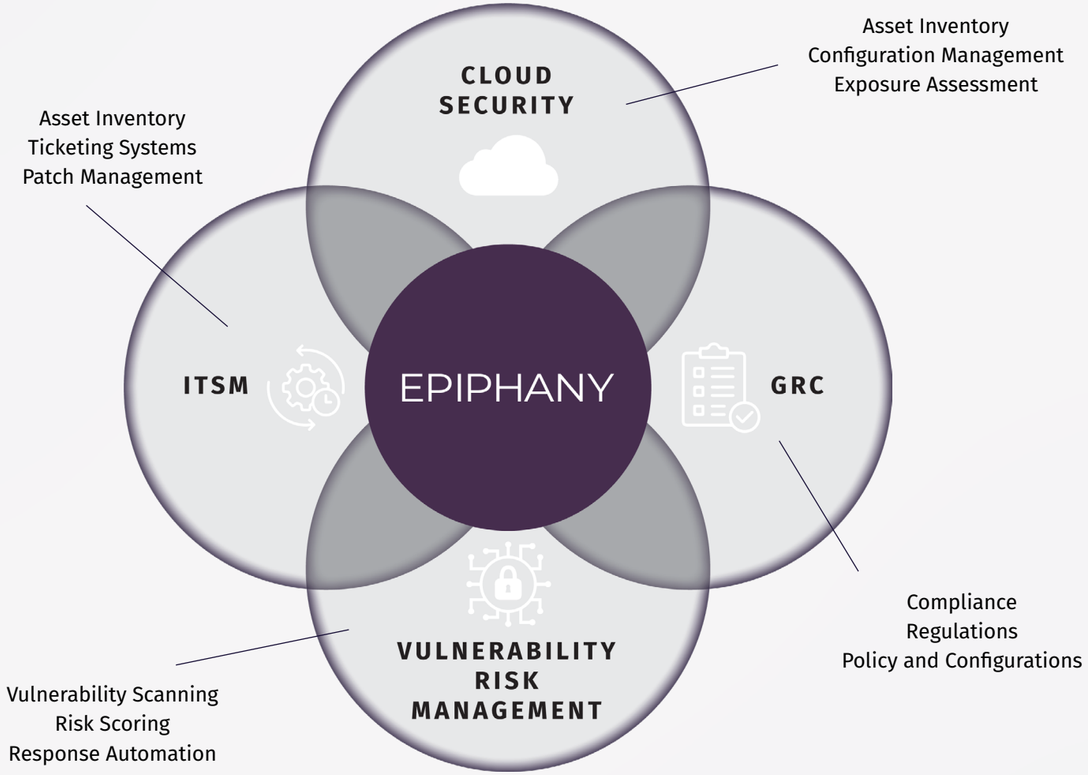
31 HUDSON YARDS, 11TH FL NEW YORK, NY 10001 (800) 794-4985 INFO@EPIPHANYSYS.COM WWW.EPIPHANYSYS.COM EPIPHANY

When it comes to reducing exposure to risk, you need to consider all three factors:

1. **What is a risk?**
2. **Would there be a material impact if that risk occurred?**
3. **What is the likelihood that it will occur?**

Weighing these three elements together shifts the focus from **vulnerability management** to **exposure management.** Redefining risk enables you to stop chasing vulnerabilities, or even exploitable vulnerabilities, and prioritize what really matters: mitigating and preventing material impact.

## Context Is Crucial




The difference between an irrelevant vulnerability and a critical threat is context. You need to understand the potential impact and the likelihood of it occurring in order to properly prioritize your risk. Time-to-context – the time it takes to evaluate context and prioritize risk – allows you to quickly resolve the issues that expose you to material impact and is essential for effective security.

Enterprise environments have variety of IT and security tools: identity management, endpoint protection, network management, vulnerability management, and more. Each of these tools contains valuable data and insight, but there is a disconnect between them that prevents you from understanding context and prioritizing risk.

The Epiphany Intelligence Platform puts cybersecurity on offense and minimizes the time-to-context. Epiphany ingests data from all available sources in your environment to build and correlate a comprehensive view of the total attack surface. Epiphany then uses artificial intelligence to evaluate your attack surface the way threat actors do to assess your environment and identify weaknesses from the perspective of the adversary.

The adversarial model finds the entry points and paths most advantageous to the attacker and identifies where you should prioritize your resources for the greatest impact. The Epiphany Intelligence Platform then provides prioritized recommendations to efficiently minimize your attack surface and manage your exposure to risk.

# Prevent Checkmate.

Consider the game of chess. Your only goal is to protect your King and prevent checkmate. Every one of your opponent's pieces is a potential risk, but at any given moment only some of those pieces are in a position where they might pose a threat to your King. You don't need to capture every piece or block every move. You just need to recognize the potential attack paths and block the moves that matter.

Effective exposure management follows the same principle. You will never patch every vulnerability. The good news, you don't have to. Your goal is not to patch or mitigate every vulnerability. It is simply to minimize and manage exposure to risk.

You don't need to address every vulnerability—just the ones that matter. The Epiphany Intelligence Platform identifies and prioritizes the ones that matter so you can proactively defend against the most critical threats to your organization.

EPIPHANY

31 HUDSON YARDS, 11TH FL NEW YORK, NY 10001 (800) 794-4985 INFO@EPIPHANYSYS.COM WWW.EPIPHANYSYS.COM

EPIPHANY

# Redefining Risk:

## Vulnerability vs. Exploitability