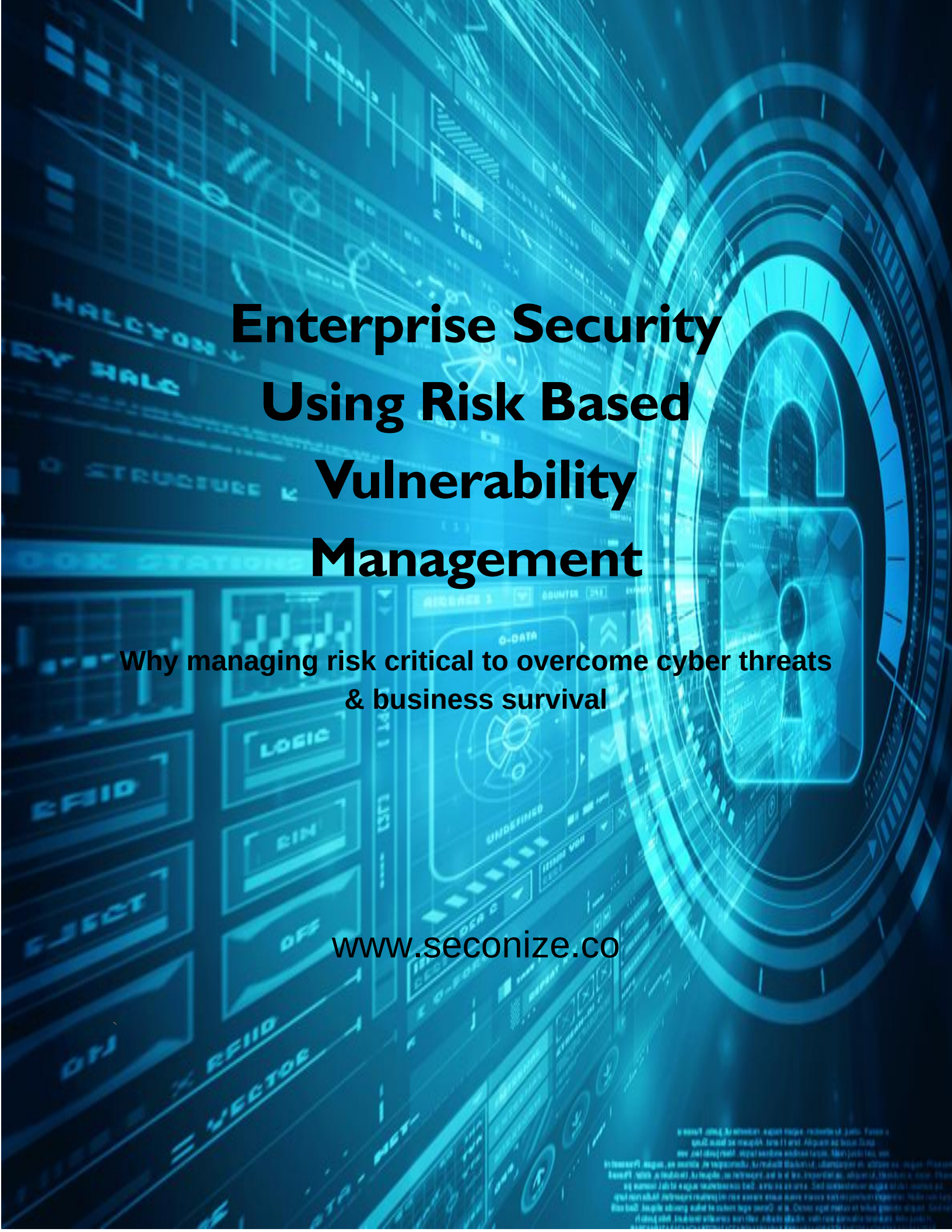


# Enterprise Security Using Risk Based Vulnerability Management

**Why managing risk critical to overcome cyber threats & business survival**

www.seconize.co

# TABLE OF CONTENTS

# INTRODUCTION

There is common saying

**“Things which matter most must never be at the mercy of things which matter least.”**

This applies very much to IT risk management and cyber security.

Most CISO, CIO heads we meet, express a common problem which is how to overcome the increasing number of cyber security issues with available resources and time.

If you look deep, we notice a common pattern that organizations are focused on addressing quantity of issues vs severity of the issues that of higher risk to their assets as well as business survival.

*2 of 5 of company’s shutdown due to Cyber Security breaches*

With organizations constrained in terms of time and money they can invest in cybersecurity, the top 3 questions that should be asked is,

1. How to ensure the focus is on addressing the risk vs compliance only?
2. How to know the security posture at near real-time vs monthly or quarterly?
3. How to be preventive and take offensive approach cyber security threats vs fixing issues and being defensive?

This article is written to address these questions and explains why organization must go beyond addressing vulnerabilities and start managing risks.

# The Growing Challenge of Enterprise Security

First lets us understand the situation in detail. The various studies from industry bodies as well as research data reveals that, there has been a sharp increase in threats in terms of opening new fronts for attack over the last few years.

**Want to know more about Risk-Based Vulnerability Management? Visit:**
www.seconize.com/demo

With the COVID, this has only increased further as organization are increasingly depended on remote working! While the world is focused on the health and economic threats, cybercriminals around the world undoubtedly are capitalizing on this crisis.

Today 85% of the Enterprise assets are in Digital format but the enterprise security is going through the biggest challenge in managing the increased cyber-attacks.

It is not just the big companies, even the SMB's are facing increased threat.

Just to give some facts,

1. $600 B is lost to cyber-attacks annually world-wide
2. $4 M is the average cost of every security breach
3. 99% of Vulnerabilities exploited will be ones already known
4. 43% of Cyber-attacks are aimed at small businesses and 60% businesses close after they are attacked

*WHO reports fivefold increase in cyber-attacks, urges vigilance*

To address these companies are trying to invest more into resources and technology.

Unfortunately, when it comes to skilled work force availability in Cyber security industry, there is shortage of 1.5 million!

## Managing risks in organizations

If we look at how businesses are responding to these increase threats, we are seeing 2 common practices are adopted.

1. Performing Vulnerability Assessments
2. Complying with industry standards

The companies have been adding more technology and tools to follow these practices diligently, but it is time to ask some questions on this with regard today's cyber security threats and sophisticated attacks.

1. Are the VA & Compliance practices future proof organizations from increased risks?
2. With constrained budgets and resources, can companies achieve increased security posture?

Let us explore in detail, why there is need to adopt to new approach?

| Category | Compliance | VA |
|---|---|---|
| Method | Manual Audits | Tool Based |
| What it covers? | Basic Compliance of standard like ISO 27001:2013, NIST-CSF | identifies vulnerabilities in assets by looking up popular vulnerability databases, like NVD (National Vulnerability Database) & From Misconfigurations |
| Limitations | Provides Only Basic Cyber hygiene<br>Requires more time<br>Increase labor requirement<br>Doesn't cover severity of any issues | Severity of the issues are based on CVSS (Common Vulnerability Scoring System), does not take the organization context into account.<br>Reports not easy to correlate and normalize for different assets<br>Too many issues identified makes difficult to prioritize |

| | | |
|---|---|---|
| Protection against cyber threats | Not sufficient | |
| Risk Based Management | Nil | Nil |
| Security Posture | Low | |

*Above all with the above methods, the 99% of the vulnerabilities exploited are already known!*

Based on this finding, two reasons can be attributed to any/most incidents:

1. The organization did not know they had the issue.
2. The organization did know they had the issue, but it got buried under tons of other issues!

So, the question is what alternative exists? This is where the issue of Risk and priority is important to consider.

Instead of being in blind spot and defensive, the top companies adopting to Risk Based Vulnerability Management

## What Is Risk Based Management?

Though cybersecurity is significant threat, investing into cybersecurity is an overhead to companies. So, it is natural, organizations are constrained in terms of time and money they can invest in cybersecurity.

Added to this, when the number of issues that are getting identified continues to increase, a new approach is required that is

1. Impact based vs checklist driven
2. Near real-time vs point in time
3. Automated vs Manual
4. Easy to interpret and unified to business goals vs technical in nature

All the above can achieved if company's starts focusing on ***managing risk.***

---

*Did you know?*

*Research has shown that organizations suffer 80% less breaches by adopting a Risk Based Vulnerability Management model.*
*- Gartner*

---

## What is risk and how to identify

The potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability.

Risk is the intersection of assets, threats, and vulnerabilities.

---

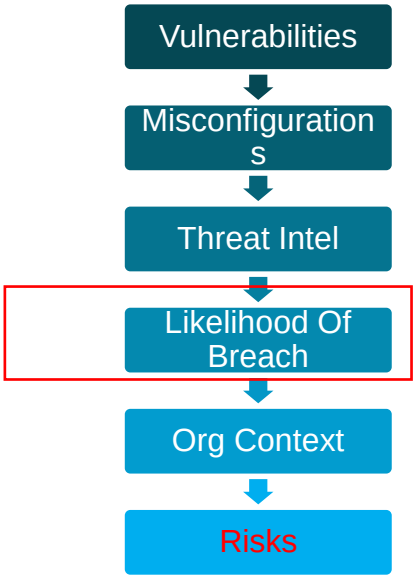
*Risk is not the enemy – too much of it is. But very importantly, so is too little of it. Between recklessness and complacency, there is a Goldilocks Zone of risk – not too much, not too little – just right.*

***Rohit Ghai - President, RSA***

---

Identification of risk involves a 5-step process that starts with Identifying vulnerabilities across the organization, model the risk for the identified weakness,

prioritize them, and start remediating the top risks – thereby given the same time and effort, the organizations is de-risking themselves optimally




## Advantages of RBVM

The advantages of risk-based vulnerability management is,

1. Automated and Continuous enterprise IT risk assessment product which
2. Evaluates the business risk for an organization vs just issues
3. It's automated and data driven approach enables easier to prioritize
4. Organization achieves an acceptable risk level and increase security posture
5. Near real-time holistic view vs point in time

**Want to know more about Risk-Based Vulnerability Management? Visit:**
www.seconize.com/demo

# Seconize DeRisk Center

Seconize is a pioneer is RVBM. With the DeRisk Center product we are helping organizations to increase their security posture across all types of asset classes.

1. DeRisk Center follows a Risk Based Vulnerability Management model.
2. Identifies asset's inherent weaknesses by performing a combination of VA, Misconfiguration checks and PT (Penetration Testing). This is the inside out view.
3. Using *Threat Intelligence* identifies the threats from the outside, outside-in view.
4. Computes likelihood of a breach for each identified weakness.
5. Further, models the risk objects and scores them.
6. Builds a prioritized risk register and suggests remediations.

To explore on how to successfully manage cyber risks,

To learn more about how Seconize can help your organization in achieving cyber security goals, visit http://www.seconize.co or book a demo call at www.seconize.co/demo

**Want to know more about Risk-Based Vulnerability Management? Visit:**
www.seconize.com/demo