tripwire

15 Myths and Risk Factors in Vulnerability Management

Tips on Avoiding Common VM Roadblocks from Cybersecurity Experts

Introduction

Vulnerability management (VM) is a much talked about practice in the IT security industry. Whether it's the debate on vulnerability scoring, how to implement a suitable VM program based on your own resources, or even trying to convince leadership a VM solution alone won't solve all your cybersecurity issues, the debate is still strong.

As one of the top three CIS Controls, VM is one of the first things that should be implemented in a successful information security program. Vulnerability management and risk management are ongoing processes—the most successful programs continuously adapt to and are aligned with the risk reduction goals of the cybersecurity program within the organization. The ongoing optimization of your VM program is essential for maintaining a reduced attack surface in your organization.

Tripwire asked cybersecurity experts to dissect the most widespread VM myths and risk factors and offer actionable advice for real VM program efficacy.

tripwire

Question #1:

What's one common myth or misconception around vulnerability management?

Myth #1: Patches always fix vulnerabilities

Many vulnerabilities are only resolved by a configuration change—Oracle's TNS Listener Poisoning vulnerability comes to mind—or they require a patch and a configuration change. Oftentimes, these configuration changes are overlooked, leaving a system vulnerable. This is why a mature vulnerability management program is so important for enterprises.

Patching with no consideration for additional steps that may be required is itself a misstep, but assuming you can tackle every vulnerability immediately is a critical mistake. It is important to realize that vulnerability resolution should be prioritized and tackled with a plan. Applying patches haphazardly can lead to improperly ordered patch installations, events which create needless work, and further strain already taxed operations teams. It is important to apply strategy to the application of patches and develop a prioritization process that works for the organization.

» **Tyler Reguly**
Manager, Software Development, Tripwire VERT
@TREGULY

Myth #2: A missing patch in itself means you're vulnerable

My favourite myth about vulnerability management is that a missing patch is equal to being vulnerable. This is not always the case. While a patch can often be a good way to remediate vulnerabilities, just because you are missing a patch doesn't mean you are necessarily vulnerable to all the vulnerabilities that patch remediates.

Instead, a VM program should look at the individual vulnerable cases to get a good idea of the asset's actual vulnerability posture. Next, it can help determine what the best means of mitigation are—not the other way around!

» **Irfahn Khimji**
Strategic Account Manager, Tripwire
@THEREALKHIMJI

Myth #3: Internal validation is enough to give you a clear picture of your cybersecurity posture

A vulnerability management program should include cyclical testing performed both internally and externally. As an example, the Payment Card Industry Data Security Standard (PCI DSS) goes as far as to require that external audits be performed by a qualified third party. An outside assessment performed by a neutral third party can validate that unbiased testing is being performed, and that the results are being correctly interpreted.

This is good advice for any organization, no matter the industry. Even organizations with relatively mature security regiments may not be utilizing both internal and external testing, and may have an incomplete view of how their security posture is evolving.

» **Ben Layer**
Principal Software Engineer, Tripwire
@BENLAYER

Myth #4: VM and patch management are the same process

A common myth about VM is that it is the same thing as patch management. While there is some overlap between the two, the goals are actually quite different. When talking about patch management, the concern is quite simply, "Do I have all the latest updates?" Meanwhile, vulnerability management specifically considers the security ramifications of misconfigured or unpatched systems.

If I were to identify the source of this misconception, I would say it's the widely held belief that all security issues are remediated by patches when, in fact, some of the most critical vulnerabilities are instead resolved by configuration changes. Ultimately, the goal of good VM is to help prioritize software updates and configuration changes based on associated risk.

» **Craig Young**
Principal Software Research, Tripwire VERT
@CRAIGTWEETS

Myth #5: It's safe to patch without verifying backups

I got 99 websites and none of them are patched. Drupal. Cold Fusion. WordPress. Internet Information Server (IIS). These are the four horsemen of VM, which only the bravest vulnerability managers confront during the cold, dark patching and updating window. It's not that these are "bad," but that they are incredibly complex software platforms and usually contain either very public web services or internally critical business systems. (In the case of IIS, these may include SQL, Exchange, SharePoint and other services.)

Not only are these platforms critical and/or highly visible, but they are also made up of a hardware or hypervisor layer, an operating system layer, a web services layer, a database layer, and hundreds if not thousands of hours of design and programming along with a myriad of customer-based or third-party add-ons and plug-ins. If something is going to go wrong, it's going to go wrong on these platforms. There is simply no platform riskier to patch and update than these production systems.

Only the foolhardy will launch patches without verifying whether a solid backup exists. If anything goes sideways like a "simple" net security update, a critical but incompatible web plug-in, or a patched library, then that system is going down hard. The myth? Patching external and internal business systems can prevent downtime. Actually, patching external and internal business systems can lead to downtime—that is, if you are not prepared to recover when a patch blows something up.

» **Ian Thornton-Trump**
Head of Cyber Security, AMTrust International
@PHAT_HOBBIT

Myth #6: All attacks rely on vulnerabilities

I think the biggest misconception around vulnerability management is that all attacks rely on vulnerabilities. While a lot of them do, and when they do they often exploit vulnerabilities for which patches have been available for quite some time, many attackers get in through the "front door," using techniques such as social engineering or weak passwords. As such, while the patching of vulnerabilities is important to reduce an organization's attack surface, it would give a false sense of security to assume that this is all it takes.

» **Martijn Grooten**
Editor, Virus Bulletin
@MARTIJN_GROOTER

Myth #7: The goal of VM is to eliminate all vulnerabilities

I think that many people have the notion that the primary goal of cybersecurity is to eliminate vulnerabilities completely. Unfortunately, VM isn't a surefire way to eliminate all vulnerabilities. At its most basic level, cybersecurity (or data security) can be expressed with a risk equation that shows risk as a function of vulnerabilities, threats and security countermeasures.

The focus is too often on vulnerabilities as if that is the only variable that can be manipulated in the risk equation. But what about the other components? What can be done to address threats? And what is left in terms of security countermeasures that are not duties related to vulnerability management? Vulnerabilities are here to stay. They will never go away nor be eliminated. VM then becomes about engaging in other activities associated with cybersecurity that go beyond just dealing with the vulnerabilities themselves.

» **Jeff Man**
Sr. Information Security Consultant, Online Business Systems
@MRJEFFMAN

Question #2:

What is a key risk factor to consider when prioritizing vulnerabilities?

Risk Factor #1: Lack of ongoing support & maintenance for assets after initial setup

One factor that is often overlooked when prioritizing risk is the support and maintainability of assets. We tend to focus on vulnerabilities, business value, and data housed on an asset—but not necessarily how maintainable the asset is going forward.

The first and largest risk factor is the lifespan of an OS and applications on the asset. For example, it's scary how many instances of Windows XP still exist in critical business areas. Microsoft ended support for this OS in April 2014 unless you reached deep into your pockets and bought extended support security fixes that were no longer available. If a new vulnerability comes out on Windows 10, you have no idea if it affects XP or even how to mitigate it, but you can bet attackers are trying exploits on XP every time.

The second factor of this risk is custom-developed software or integrations. Many times, these were developed by contractors, professional services, or even internal developers who have moved on, leaving no one to maintain them. Almost every organization has a system that runs fine but cannot update it because a new version breaks the usage and no one knows how to fix it. The last factor is maintenance and updating hardware, because security is not just limited to the software on the asset. Processors, network cards, system BIOS, and RAID cards are all targets to exploit, and we tend to have an "if it ain't broke, don't fix it" attitude toward these. In many organizations, firmware versions are not even tracked let alone updated.

» **Lamar Bailey**
Sr. Director, Security R&D, Tripwire
@BTLE310

Risk Factor #2: Failure to identify the level of business risk posed by individual assets

One area where I see many organizations are struggling is their failure to not only identify what assets are on their network but also assess the risk of those assets and determine what type of risk they pose. Does an asset have PII or other sensitive data, or is the asset critical to business continuity?

This process is a challenge for security and IT organizations primarily due to the fact that it is often not a technical exercise but more a business process and collaborative effort as it requires input from business leaders and stakeholders across the organization. However, once this work is done, it provides much more context for security teams to prioritize vulnerabilities and provides incident responders with a better understanding of a given threat.

» **Ken Westin**
Security Analyst, Director, ITOA & Security Solutions at Elastic
@KWESTIN

Risk Factor #3: Some vulnerabilities are brought on by business processes and decisions

Business is a key factor in assessing vulnerabilities and their risks. No one chooses the vulnerable library on purpose; no one chooses the out-of-date server version because they want to be exploited. There are deep business reasons why something is the way it is. For example, a tech company may have initially chosen one language for the front end—but when they had developers leave, a lack of skills led to choosing a new language out of necessity.

» **Haydn Johnson**
Information Security Manager, Points
@HAYDNJOHNSON

Risk Factor #4: Some assets are more critical than others—know what you need to protect most

I think of crown jewels (digital crown jewels, that is) as key factors when prioritizing vulnerability risk. What is your most valuable asset that you cannot replace or cannot risk the loss of? This could be intellectual property, proprietary applications and software, and/or very sensitive data. Think like a ruthless rival or attacker. What would you take or break to bring your organization down?

» **Cheryl Biswas**
Strategic Threat Intel Analyst, Cyber Security at TD
@3NCR1PT3D

Risk Factor #5: Make sure to integrate VM into the IT and business processes of the organization

I would say that there are multiple key factors for a VM program to be successful.

The first thing we need to understand is that It is impossible to remediate all the vulnerabilities for all assets in an enterprise. Before we think and plan for vulnerability remediation, we must figure out what is important for the business. Once critical assets have been identified, the IT security team should get serious about scanning and remediating vulnerabilities that pose the highest risk to the organization. Not only must it select a strong scanning tool, but the organization should also add a cross-functional set of people who can help you understand the potential risks.

The next step is to aggregate all data in a tool that can help you prioritize and manage the vulnerabilities. Adding threat intelligence and automation is always a good practice when working on the centralized tool. Next, document the program and get agreement from all stakeholders to start your cycle. Finally, communicate to management and executives, focusing on the highest risks and the actions that need to be protected. As the program evolves, vulnerability risk management becomes a natural part of the IT processes in the organization.

» **Rafael Garcia**
Senior Information Security Consultant
@RAFUCA

Risk Factor #6: Multiple critical vulnerabilities require a balancing act that takes the big picture into account

To be perfectly honest, there are a lot of them. Assuming we're looking at a report in which a severity rating has already been assigned to each finding, it goes without saying that the highest-severity issues should be tackled first. With that said, if you're staring down the barrel of multiple critical vulnerabilities, sometimes it makes sense to perform triage.

Fix the easy stuff first, then worry about tackling the remediations that require more time or resources to implement later. You'll reduce your attack surface faster that way. However, this isn't a hard and fast rule—you also need to consider the vulnerability's potential impact on the organization when making these kinds of decisions. It's a balancing act.

» **Gabriel Ryan**
Principal Consultant
@S0LST1C3

Risk Factor #7: It's crucial to think of vulnerabilities in terms of consequences of exploit

If a vulnerability exists in an entity which a large number of people use, whether it's an application, device, a software development library, or whatever, I would consider what the worst possible consequences would be if it was exploited. For example, a vulnerability which can be exploited to expose the financial data of millions of people should be prioritized over a vulnerability which could be exploited to spoof PlayStation Network trophies.

Both vulnerabilities are important to mitigate, but the financial vulnerability could have much more dire consequences if attackers could exploit it. Any applicable industry and government regulations—such as PCI DSS or GDPR—should also be considered when prioritizing vulnerabilities to focus on.

» **Kim Crawley**
Cybersecurity Writer
@KIM_CRAWLEY

Risk Factor #8: Don't just rely on CVE value when tackling vulnerabilities

When a known vulnerability is discovered, many will start with the CVE value. This metric is still important as it can define ease of exploitation, and it provides a starting point. However, in a world where security is now business driven and security is no longer binary, environmental factors including business context must be considered to provide the overall risk (residual) value. This is key when trying to convey the value and impact to company stakeholders.

Companies must have visibility into their network and know the value of the information they are protecting. While key factors such as understanding the complexity of the attack vector are important, there must be a joining of security and business context driving the prioritization.

» **Lidia Giuliano**
Information Security Professional
@PINK_TANGENT

Tripwire Can Help You Create a Mature VM Program

Strengthen your vulnerability management program with Tripwire® IP360™, the VM solution with the industry's most granular risk scoring system and lowest false positive rate.

Learn More

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at** tripwire.com

***The State of Security*: News, trends and insights at** tripwire.com/blog
Connect with us on LinkedIn, Twitter **and** Facebook

 BRMRFVM1a 1905