REPORT

2017 Outlook: Vulnerability Risk Management & Remediation Trends

NOPSEC

nopsec.com | hello@nopsec.com

Table of Contents

Introduction

This year's respondents represent a cross section of ten industries including government, healthcare, financial services, energy, food and beverage, and others.

For the second year, NopSec presents top findings from our annual survey of IT and security practitioners. Our goal is to provide a snapshot of the current state of vulnerability risk management (VRM) and challenges that impact the remediation process in organizations. We also present findings about how information security (infosec) teams measure success in their organizations, how they view the level of understanding among their senior leadership when it comes to cybersecurity programs, and finally, their priorities for improving VRM in the coming year. This year's respondents represent a cross section of ten industries including government, healthcare, financial services, energy, food and beverage, and others. Just under half (46%) are at the director or chief level in their organizations. Thirty-eight percent are managers, and sixteen percent report being in junior level positions.

To begin, we share IT leaders' responses regarding their overall approach to VRM and the scope of their VRM programs. Many of the trends are encouraging, while others demonstrate room for improvement. In the latter case, we provide our recommendations for any organizations that find themselves facing the same circumstances and challenges as our respondents. As we look closer at the possibilities for the year ahead, tech leaders' answers to some questions reveal an opportunity for more organizations to benefit from VRM technology that can help solve some of your most common challenges. We also continue to see room for growth when it

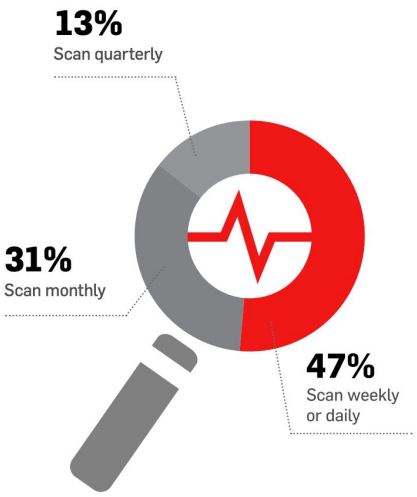
comes to executives' and other stakeholders' understanding of cybersecurity. At the same time, infosec leaders are motivated to make improvements, and they identified key priorities for enhancing their VRM programs in the coming year.

Current Trends in Vulnerability Risk Management

Many Companies Remain At Least Partially Compliance-Driven in Their Approach to VRM

With 16% of respondents saying that VRM is a function mostly driven by compliance requirements, and almost half (47%) saying that their VRM is equally driven by both compliance and security risk management, there is room for many companies to move away from a compliance-driven mentality. While compliance will remain an important driver, particularly for industries like financial services and healthcare, compliance alone does not keep organizations secure. When VRM is a strategic practice that is part of your overall security and risk management strategy (true for 36% of those surveyed), then your business priorities are more likely to be aligned in a way that provides adequate resources, time, and attention to minimize security risks. Moreover, organizations that are strategy-driven will find it easier to remain compliant for these same reasons.

The Vast Majority are Scanning for Vulnerabilities Quarterly or More, But Only About Half Scan All or Nearly All of Their Environment on a Regular Basis



A scan should also be completed any time new equipment or applications are installed, and scans should be repeated until they show that the most critical vulnerabilities have been addressed.

As regulations like HIPAA and PCI typically call for scanning four times per year to remain compliant, it's not surprising that most respondents report at least quarterly scanning. Thirteen percent say they are right at the quarterly mark, while another 31% are scanning once per month. An additional 47% scan more often (weekly or daily). In all, almost 91% of survey respondents report scanning quarterly or more. And while 56% of respondents report scanning 75-100% of their entire environment on a regular basis, this means that nearly half are regularly doing only partial scans.

If you are among that latter half, we recommend that you move toward having your entire environment covered by the scope of your scans. Although there are instances when partial coverage is enough, these are exceptions – it's best if the rule in your organization is to do full scans. A scan should also be completed any time new equipment or applications are installed, and scans should be repeated until they show that the most critical vulnerabilities have been addressed.

A Significant Number of Companies Continue to Rely on Manual Prioritization and Limited Inputs to Prioritize Vulnerabilities

One quarter of respondents rely either solely on CVSS scores to prioritize vulnerabilities (11%), or they use a combination of CVSS scores and asset classification (15%). Most infosec

professionals recognize that CVSS scores alone are insufficient, but even adding only asset classification leaves organizations at risk and doesn't do enough to minimize data overload.

Organizations should apply all the information they can find to prioritizing vulnerabilities. That includes CVSS scores and asset classification, but also threat intelligence, exploit feeds, social media trends, patches available, and business context. This is incredibly difficult to do manually. It also drains resources from other activities, which results in opportunity costs for organizations operating with small IT teams that wear many hats. Automating prioritization using technology that can incorporate all of the factors listed above is the best answer to overcoming this challenge.

Similarly, when asked, "What types of threat intelligence are used within your vulnerability risk management program?" 29% of those surveyed told us they don't use any threat intelligence feeds, while another 26% rely on open source feeds. Open source feeds are insufficient alone – a combination of open source and commercial feeds should be used. In addition, organizations can usually save money and time by implementing a VRM platform that incorporates multiple feeds for them. For instance, Unified VRM integrates threat intelligence from FireEye, SANS, Exploit Database, AlienVault, and Team Cymru. The cost to users for these feeds is less than it would be by buying all of them separately, and the technology eases the research process for IT staff.

Emphasis on Remediating External Network Infrastructure Suggests a False Sense of Security Among Some Organizations

Starting with the good news: 42% remediate critical vulnerabilities in external network infrastructure in under seven days. However, many organizations mistakenly think that external networks are the most vulnerable, while motivated attackers know that there are other ways to penetrate a network beyond external-facing entry points.

Responses suggest that companies tend to be more lax when it comes to internal network infrastructure and web applications. It's best to remember this old adage of perimeter security: a hard core on top of a soft shell. This approach does not work anymore in an environment where the security's last frontier is the endpoint security. Thirty-one percent report remediating critical internal network vulnerabilities in under seven days, and the number is slightly higher for web applications at 35%. Companies sometimes think that "internal" means safer, but in reality, attackers go for these networks the most because they are usually the quickest paths to access everything else of value – from the CEO's email to the company's proprietary data to customer data.

The Biggest Challenges to Data Prioritization Can Be Addressed with the Right VRM Technology

When asked about their biggest challenges to data prioritization, three responses topped the list: lack of budget (27%); data

overload (24%); and lack of resources/too much manual time spent (20%).

The good news is that with the right VRM technology, all three of these challenges can be addressed. Many companies shy away from investing in good VRM platforms because of budget concerns, but investing in the right tools means you maximize your return on investment by allocating resources better. Technology that is a fit for your business and that helps you prioritize and enrich data properly (the basis of all remediation) can save you staff time (and therefore money and opportunity costs) on the manual prioritization your team is already doing. It can also incorporate threat intelligence that your team could never possibly have the time and ability to correlate manually.

Looking at the cost of a solution holistically gives you a better sense of the importance of the investment. For instance, NopSec's Unified VRM not only addresses all three of respondents' top challenges. It also can save users money on threat intelligence feeds; the feeds that Unified VRM integrates with would cost up to $750,000 every three years if they were to be purchased separately.

The Biggest Impacts on the Remediation Process are Addressable with the Right Technology, Too

Respondents rated nine common challenges to the remediation process according to their impacts, and the biggest issues stood

out as ones that, like data prioritization challenges, could be addressed with the right technology.

Lack of resources to get the work done was the top challenge, and was followed by its frequent corollary in organizations that have teams responsible for multiple aspects of the IT department: competing priorities with other operational demands.

Time spent on manual assessments as well as false positives and/or validity of vulnerability findings were the leading technical challenges that teams reported to have a moderate impact on their remediation process.

The right VRM technology goes beyond what the average scanner does to eliminate the "noise," like false positives and duplicates, common to raw data scans. It does so in an automated way that reduces the time that staff must spend on manual work. Combine this with good ticketing, workflow, and reporting capabilities, and a quality VRM platform will effectively ease the most common remediation issues.

Executives and Other Stakeholders are Playing Catch-Up When It Comes to Understanding Cybersecurity

About a third – 29% – of respondents characterized executives and key stakeholders in their organizations as "fairly" or "very well" informed about security threats. That makes the rest of

leaders and stakeholders “average” (53%) or less (18%) when it comes to their understanding.

Cyber threats are ever-evolving (as they will continue to be), and even wise business leaders are playing catch-up on cybersecurity’s importance to privacy and infrastructure. As the responses to other survey questions validated, a good information security program requires resources and support. Without executive support, infosec teams struggle to obtain budget for the right tools, hire the right resources, and invest in training and education that must happen across the organization to address the biggest security weakness anywhere, the human element. All of these things only come to the IT team if executives and other stakeholders have a firm understanding of the infosec program’s strategic business importance. Responses to this question show that more can be done to increase that understanding.

(For tips on obtaining management support for your VRM technology investment, download our guide: “Secure C-Suite Buy-In for an Information Security Platform.”)

Use of Metrics is Relatively Common, But Shows Room for Growth

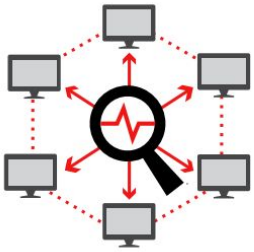
Forty percent of our survey takers responded in the affirmative when asked whether their organizations use metrics to measure the success of their VRM programs. About half (53%) said they do not use metrics, and 7% don’t know. If you are not already

using metrics to manage your VRM program (or if you are but you want to be sure you are measuring the right things), we recommend starting by getting a baseline measure of these key metrics so that you can begin to set goals and track improvements to your VRM program over time.

24%
implement tools to improve prioritization

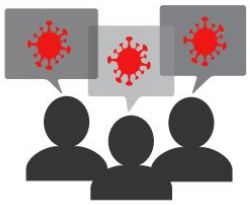
The Vast Majority of IT Organizations Know They Can Improve Their Remediation Processes

Only about 16% of respondents believe the current state of their organization's remediation process needs little or no improvement. Meanwhile, roughly 84% see room for "some improvement" (51%) or "major improvement" (33%).



22%
scan networks more frequently

When asked about their priorities for improving their VRM programs in the next 12-18 months, three things top the list: implement tools to improve prioritization (24%); more frequent scanning (22%); and implement goals and success metrics to reduce remediation time (20%).



20%
implement goals and success metrics to reduce remediation time

Implementing prioritization tools is number one for good reason. Your security process depends on the quality of information telling you which vulnerabilities need your attention the most and which remediation efforts will deliver the most positive impact. As already recommended, the other two leading priorities are also top actions we would like to see in 2017 for those organizations not doing full, frequent scans and/or using success metrics to optimize their programs.

When you are up against a fast-changing environment, increasingly sophisticated and malicious attackers, difficulty acquiring great IT talent, budget constraints, and competing business priorities, maintaining 100% cybersecurity may not be a realistic goal. However, keeping risk to an acceptable minimum is possible. The outlook for VRM across industries shows opportunity for addressing the most common challenges by increasing awareness and implementing the right technology

Find out how NopSec's Unified VRM can help you think like a hacker and stay ahead of the trends. Visit www.nopsec.com or email hello@nopsec.com for additional information or to request a demo.

About NopSec

NopSec operates with one mission: to help people make better decisions to reduce security risks. Our team is passionate about building technology to help customers simplify their work, manage security vulnerability risks effectively, and empower them to make more informed decisions. Our software-as-a-service approach to vulnerability risk management offers an intelligent solution to dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation.