REPORT

2018 Remediation and Vulnerability Risk Management Trends

NOPSEC

nopsec.com | hello@nopsec.com

Table of Contents

Introduction

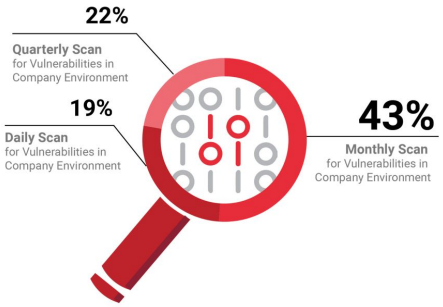
NopSec presents top findings from our third annual survey of IT Security and Risk practitioners. The goal of the survey is to provide a snapshot of the current state of vulnerability risk management (VRM) and challenges that impact the remediation process within organizations. The report presents current findings of how information security (infosec) teams measure vulnerability management success, the perceived level of understanding among senior leadership when it comes to cybersecurity programs, and finally, priorities for improving VRM in the coming year.

This year's respondents represent a cross-section of diverse industries including healthcare, financial services, education, retail, food and beverage, and others. Approximately 37% of respondents are at the director or chief level in their organizations, 37% are managers, 24% reported being in junior level positions, and 1% reporting as other. It is important to note that our analysis comes from a sample of clients and professional contacts – as such, we do not claim that this is a definitive analysis of vulnerability risk management and remediation trends an average organization could face.

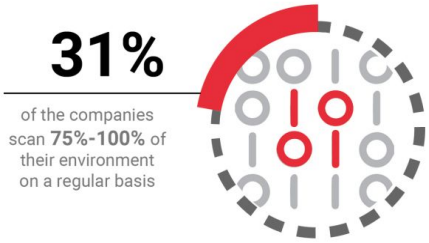
To begin, we share the responses of IT professionals regarding their overall approach to VRM and the scope of their VRM programs. Many of the trends are encouraging, while others demonstrate room for improvement. In the latter case, we provide recommendations for any organizations that find

themselves facing the same circumstances and challenges as our respondents. As we look closer at the possibilities for the year ahead, tech practitioners' answers to some questions reveal an opportunity for more organizations to benefit from VRM technology that can help solve some of the most common challenges. We continue to see room for growth with regards to understanding of cybersecurity by executives and other stakeholders. At the same time, infosec leaders are motivated to make improvements, as they identified key priorities for enhancing their VRM programs in the coming year.

Only 31% of Organizations Scan 75-100% of Their Environment on a Regular Basis



Many organizations (43%) report that they are scanning their environments on a monthly basis. This is an increase in the number of monthly scans taking place compared to last year at 31%. We also found that fewer organizations scan for vulnerabilities on a daily basis, down from last year's 24% to 19%. This might be concerning news to some, but it is not surprising to learn that organizations have been scanning less often while infosec professionals also stated that data overload is a key issue facing organizations today.



As an indicator of industry wide appreciation in the value of VRM, 93% of all survey respondents report scanning quarterly or more. This is likely due to compliance regulations, such as HIPAA and PCI, which require organizations to perform vulnerability scans on a quarterly basis. What is surprising, however, is that only 31% of respondents report scanning 75-100% of their entire environment on a regular basis, and more than half (69%) are only performing partial scans.

It is best practice to perform full environment vulnerability scans on a regular basis. Scans can take a long time and vulnerabilities detected can be difficult to prioritize making the process of total environment scanning overwhelming to some. Network scans should include all devices with an IP address (workstations, laptops, printers and multifunction printers, routers, switches, hubs, IDS/IPS, servers, wireless networks and firewalls) and all

the software running on them. New scans should also be performed any time new equipment or applications are installed or in the event of significant architecture updates. Scans should be repeated until they show that the most critical vulnerabilities have been mitigated. Furthermore, performing scans on 100% of the assets within an environment allows organizations to detect threats that may have otherwise been overlooked.

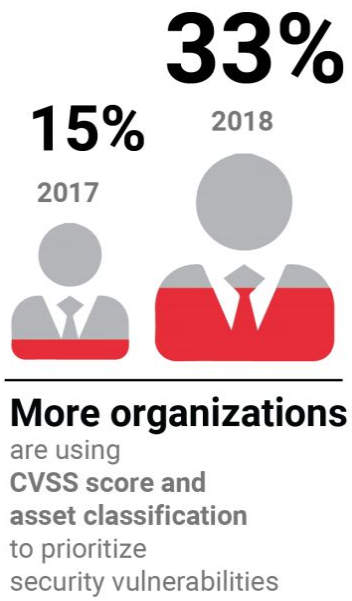
Organization's Vulnerability Risk Management is Currently Driven by Compliance and Security Risk Management

The introduction of new and updated regulations such as NYDFS (23 NYCRR Part 500), PCI DSS 3.2, and GDPR (Regulation (EU) 2016/679) have sparked new conversations and focus around enhancing cybersecurity policies to meet these regulations. In fact, 31% of respondents said that VRM is a function mostly driven by compliance requirements, while another 39% said that VRM is equally driven by both compliance and security risk management. Overall, there has been a notable increase in compliance-driven VRM with 70% of all respondents factoring compliance into their VRM program compared to 63% of last years. Compliance frameworks and regulatory controls have merit. However, simply meeting compliance requirements leaves organizations at risk. Standards are typically set in an attempt to force organizations to play catch up with the evolving threat environment[1] due to disruptive trends, such as the increased frequency and magnitude of data breaches . Implementing

[1] ITRC "At Mid-Year, U.S. Data Breaches Increase at Record Pace" July 2017

compliance initiatives along with an ongoing, proactive, inclusive cybersecurity program provides a more comprehensive approach to vulnerability risk management. Promoting cyber hygiene in addition to industry best practices are essential for mitigating advanced threats.

Most Organizations Prioritize Vulnerabilities with a Combination of the CVSS Score and Asset Classification

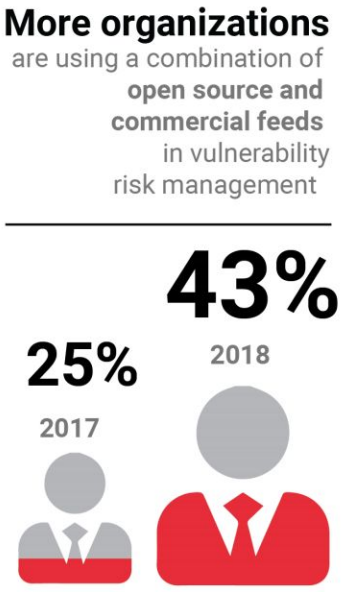


Over the years many infosec professionals have recognized that the Common Vulnerability Scoring System (CVSS) alone is not sufficient for vulnerability prioritization[2]. We've seen an increase in the number of respondents using a combination of CVSS scores and asset classification (33%) compared to 2017 numbers (15%). The use of manual correlation in vulnerability prioritization has remained constant at 29% since 2017. Manual prioritization can be error-prone and creates delays in the vulnerability remediation process, thereby increasing risk. Additional tools and resources such as AI, Machine Learning, and threat intelligence can add valuable insights into vulnerability prioritization.

[2] CSO Online "How to get CVSS right" April 2015

Open Source and Commercial Feeds are the Most Common Types of Threat Intelligence for Vulnerability Risk Management Programs

The prioritization of vulnerabilities has proven to be a difficult task for many cybersecurity teams[3]. When deciding which vulnerabilities to remediate first, organizations should arm themselves with as much contextual information as possible. Analyzing information, such as threat intelligence, exploit intelligence, available patches, social media trends, and individualized business context in addition to CVSS scores and asset classification will provide cybersecurity teams with a more comprehensive view of vulnerability risks.



Encouragingly, more infosec professionals have begun to recognize the importance of using threat intelligence in their vulnerability risk management program. We found that 94% of respondents are using at least one type of threat intelligence feed. More encouraging is that 43% of respondents are using a combination of open source and commercial feeds, which is an 18-point increasing compared to last year.

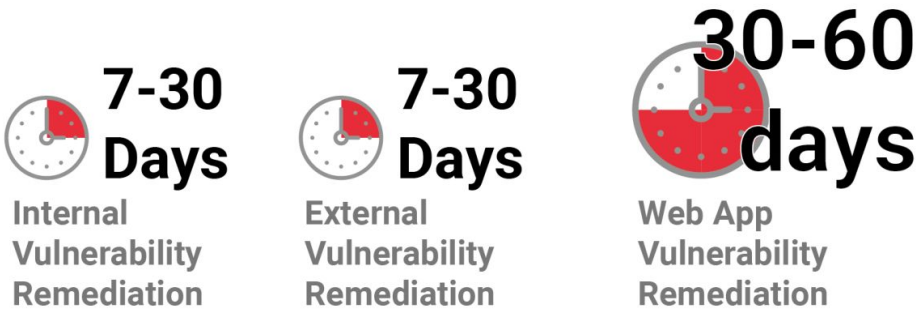
Threat-centric vulnerability remediation helps organizations to analyze true risk and gradually reduce said risk. We recommend using more than one threat intelligence feeds to maximize insight and contextualization of your organization's vulnerability risk.

[3] NetworkWorld "Three key challenges in vulnerability risk management" September 2015

It may be challenging for some organizations to purchase multiple threat, exploit, and vulnerability intelligence feeds depending on the bandwidth of their organization's cybersecurity program. Implementing a vulnerability risk management tool which aggregates these kinds of sources may be a solution. Unified VRM has multiple threat, exploit, and vulnerability feeds embedded in its E3 Engine, from a variety of sources such as AlientVault, Symantec, and Twitter. By aggregating multiple vulnerability data sources cyber security teams are able to be more efficient while managing risk within their organizations.

Critical Web App Vulnerabilities Take the Longest Amount of Time to Remediate at an Average of 30-60 Days

We found that on average it takes cybersecurity teams 7-30 days to remediate vulnerabilities within organizations' external and internal networks. Comparatively, these teams spend at least twice as long to remediate web application vulnerabilities, with the majority of respondents reporting that it takes 30-60 days on average.



This is a concerning trend considering that web application vulnerabilities can pose just as much danger as vulnerabilities within internal or external environments. Especially since the more time spent on remediation leaves a longer window of exposure for vulnerabilities. It is also essential to consider the level of complexity in web application remediation, and cybersecurity teams should look for additional resources and tools to help shorten the time spent on this process.

Even though the level of work required for remediation varies on a case by case basis, it is valuable for organizations to remember that internal, external and web application vulnerabilities can all be entry points for malicious actors. Therefore remediation of each should be addressed with equal importance within an organization's vulnerability risk management program.

Data Overload, Lack of Resources, and Lack of Relevance are the Top 3 Challenges Facing Vulnerability Risk Management Teams

When it comes to vulnerability prioritization, respondents identified the biggest challenges they're facing in 2018 as, data overload (32%), lack of resources (22%), and lack of relevance (17%). Specifically, data overload refers to the immense amount of vulnerability data to prioritize, lack of resources refers to the laborious amount of time spent enriching the vulnerability data, and lack of relevance refers to the insufficient insight on the vulnerability data pertinent to the environment.

It is encouraging to report that more organizations are allocating sufficient budgets to cybersecurity programs compared to the results from 2017's Vulnerability Management and Remediation Trends Survey. The number one challenge facing the organizations last year was "lack of budget" with 27% of respondents, but this year only 5% of respondents indicating that they are facing the same issue during their vulnerability prioritization process. Budget alone does not solve all VRM challenges, but spending on certain tools can help to minimize them.

Nevertheless, it should be noted that data overload and lack of resources are still top challenges facing infosec professionals when prioritizing vulnerability scan results. More industry professionals (17%, compared to 11%) are naming lack of relevance as a top constraint in the process of prioritizing their vulnerability data.

Lack of Understanding of the Risks Posed by Security Vulnerabilities Has the Most Negative Impact on the Remediation Process

Infosec professionals were asked to rank various challenges that they face during the remediation process based on the level of negative impact. The top two challenges identified by organizations are the "lack of understanding of the risks" posed by security vulnerabilities and the "lack of resources available to

get the work done". False positives and/or the validity of vulnerability findings were cited as the third most impactful challenge to the remediation process.

"Lack of resources" and "false positives" were also identified as top challenges in 2017's survey. Unfortunately, "chronic data overload", "error-prone manual processes", and the "shortage of cybersecurity talent" continue to pose challenges to the status quo. The "chronic data overload" in VRM teams and "time spent on manual vulnerability prioritization" introduces errors, delays, and risks that represent major impacts on their remediation process. The "skills and expertise gap" further the problem as IT Security teams lack both the insight and the manpower to address these challenges.

The right VRM technology alleviates these major issues in an automated way, thereby reducing the time that staff must spend on manual work. Combining this with good ticketing, workflow, and reporting capabilities, the UVRM platform will effectively ease the most common remediation issues.

Nearly One-Third of Respondents Do Not Have Metrics in Place to Measure the Success of Their Vulnerability Risk Management Programs

When asked whether their organizations use metrics to measure the success of their VRM programs 69% of our survey

respondents confirmed that they do, but about a third (31%) said they do not use metrics.

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.

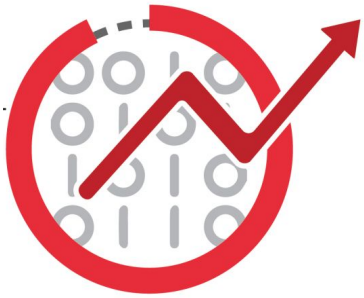
Key metrics to watch out for would vary depending on the goals of your organization. CISOs and Managers, for example, will look for more global visibility metrics including overall security posture, industry benchmarks, and performance. Engineers and Analysts will be looking for more granular metrics such as ticket aging and vulnerability trends.

NopSec's Unified VRM provides dashboards to view these global metrics and helps IT Security stakeholders view the same

metrics in different contexts relevant to their goals. In addition, the platform also provides reporting capabilities.

Integration with SIEM or Incident Response Systems are Top Priorities for Improving Vulnerability Risk Management Programs in 2018

When asked about their priorities for improving their VRM programs in the next 12-18 months, three things top the list: integration with asset and/or configuration management systems (22%); integration with SIEM/incident response systems (22%); and implement tools to improve prioritization of vulnerabilities and threats (16%). These results are different from last year that are more task-driven (scanning) and shows a shift into strategic integrations for a more agile VRM automation and orchestration process.



93%

of respondents see room for "some improvements" to "needs major improvements" in their organization's remediation process

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 percent cybersecurity may not be a realistic goal. However, keeping risk to an acceptable minimum is achievable. The outlook for VRM across industries shows opportunity for addressing the most common challenges by increasing awareness, addressing the chronic problems faced by IT Security and Risk Team everyday, and implementing the right technology to support them.

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.

NopSec helps security professionals simplify their work, effectively manage and prioritize vulnerabilities, and make better informed decisions.

NopSec's Unified VRM is an innovative threat and vulnerability management solution that addresses the need for better prioritization and remediation of security vulnerabilities in a single platform.

NopSec Inc. • www.nopsec.com • info@nopsec.com