REPORT

2016 Outlook: Vulnerability Risk Management and Remediation Trends

NOPSEC

nopsec.com | hello@nopsec.com

Table of Contents

Introduction	2
Current Trends in Vulnerability Risk Management	3
Putting Management in Vulnerability Risk Management	6
2016 Outlook: Priorities in Vulnerability Risk Management	8
About NopSec	10

Introduction

The practice of vulnerability risk management is not new. Every information security control framework requires organizations to perform some level of regular vulnerability assessment. Most organizations – from SMEs to enterprises – are doing just that. Today, nearly 70% of organizations scan some portion of their environment for vulnerabilities at least weekly.

Vulnerability risk management has become a numbers game, with more than 50% of organizations citing data overload as their biggest challenge to effective vulnerability prioritization. The CVSS scoring system, originally launched in 2004, was developed as a method to quantify the severity of security vulnerabilities and give organizations a basis for determining risk across their environment. More than a decade later, data breaches continue to be rampant and organizations still struggle to effectively prioritize vulnerabilities and make the move to remediation faster.

A recent investigation into the 2013 Target incident, where tens of millions of payment cards were stolen and breach damages were expected to reach $148 million[1] , demonstrates the essence of everything that is wrong with current vulnerability risk management practices. The Verizon report[2] noted that Target "had a comprehensive vulnerability scanning program in place," however, lacked robust procedures to remediate identified weaknesses in a timely manner. This finding comes as no

[1] Time Magazine, "Target Expects $148 Million Loss From Data Breach," August 2014
[2] Krebs On Security, "Inside Target Corp., Days after 2013 Breach," September 2015

surprise when 82% of organizations indicate their current remediation process is broken.

60% of respondents stated company executives are only "somewhat" to "not at all" informed about the risk posed to their business from today's security threats.

This report, based on responses from nearly 200 IT and security practitioners surveyed, explores the current state of vulnerability risk management, the challenges that directly impact the remediation process, and the outlook for improvement in the coming year. In addition, compliance drivers and executive awareness of information security threats are considered to demonstrate their influence on effective vulnerability risk management.

Current Trends in Vulnerability Risk Management

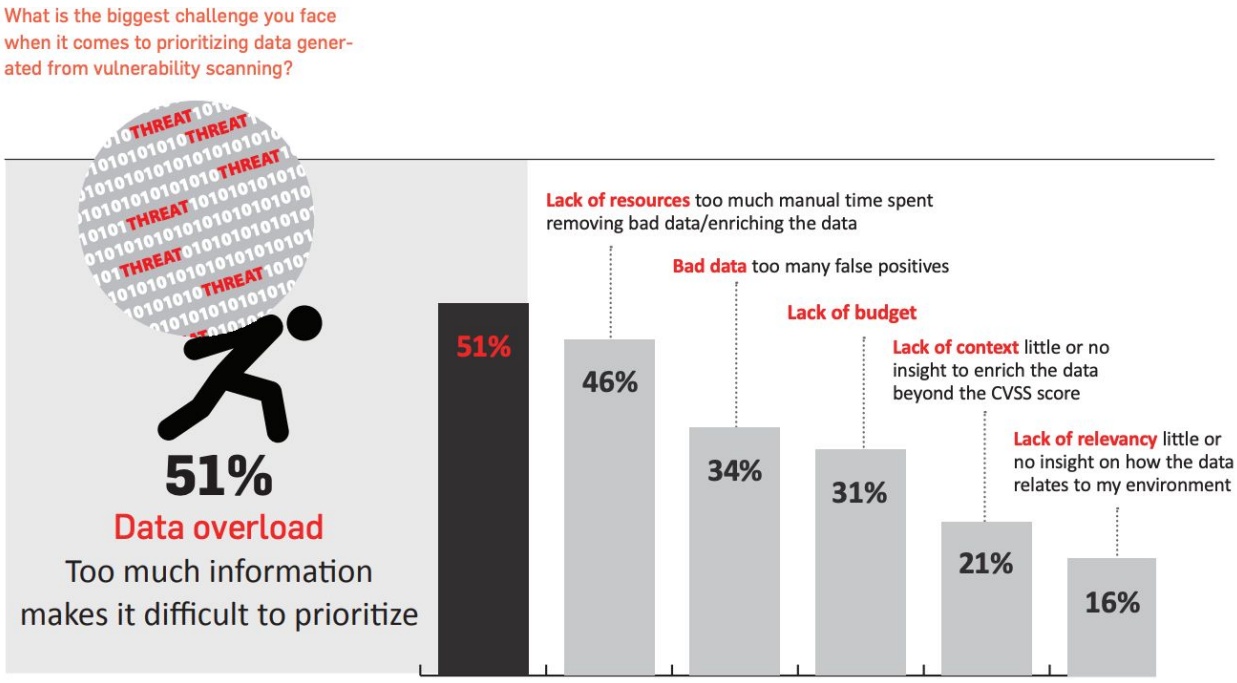
Security vulnerabilities are multiplying at alarming rates. There is a new security vulnerability identified approximately every 90 minutes, and an average of seven vulnerabilities per asset across the IT environment[3] . Vulnerability risk management has become a numbers game, only further exacerbated by the expansion into cloud and mobile technologies. Today, organizations are very actively detecting threats across their environment. According to respondents, nearly 70% are scanning their environment on a daily or weekly basis, and 41% are scanning at least three-quarters of their IT assets for vulnerabilities.

Vulnerability scanners provide the visibility into the potential risk land mines across the network, applications and endpoints. But

[3] NopSec, "2015 State of Vulnerability Risk Management," June 2015

the question of what to do next has created an overload of data tracked in spreadsheets, inefficient business processes, and communication breakdown between internal teams in charge of remediation.

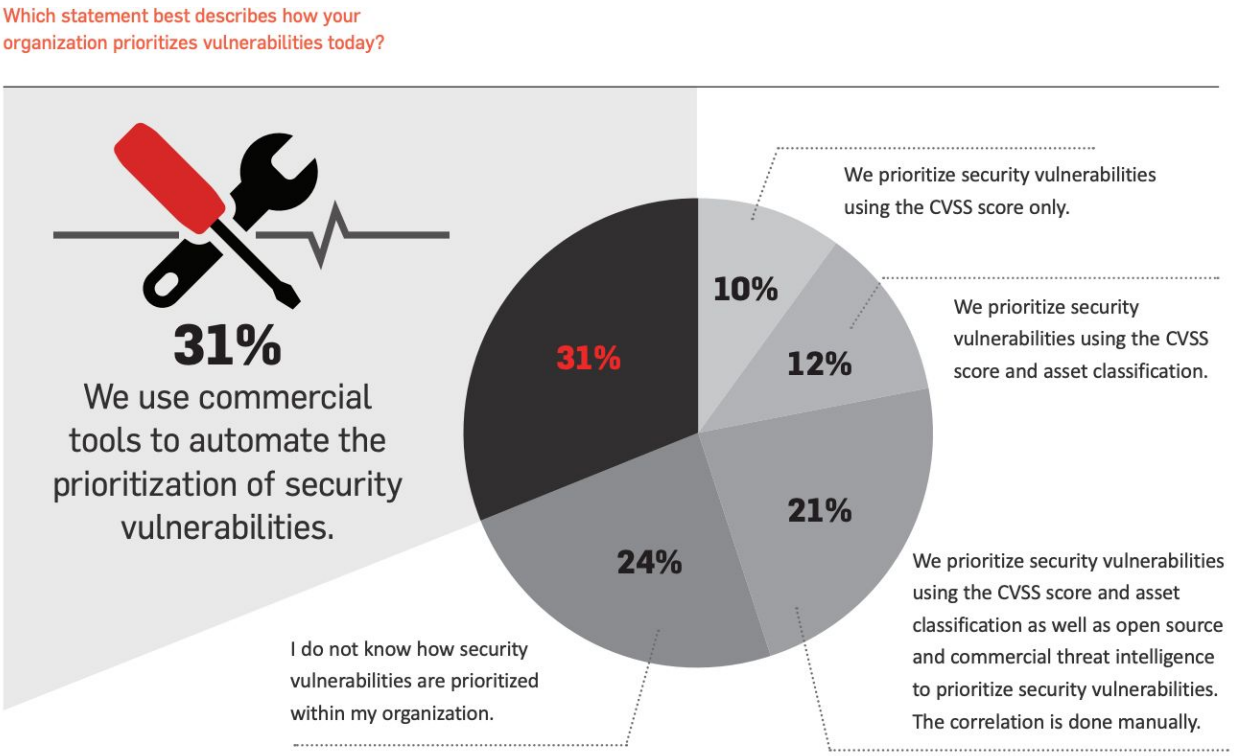
Despite active detection, the internal teams tasked with remediation and risk management are still faced with sifting through an avalanche of data (see Figure 1). In fact, more than half (51%) of organizations surveyed cited data overload as their biggest challenge to prioritizing data generated from vulnerability scanning, followed by lack of resources (46%) and too many false positives (34%).



Not all vulnerabilities are created equal. While the Common Vulnerability Scoring System, or CVSS score, provides a basis for organizations to begin the process of prioritizing threats, it is by no means the best measurement of risk on its own. Factors such

as known exploits, active malware attacks, available patches, and the criticality of an asset also need to be considered.

Organizations do, however, recognize the value of this additional context to prioritizing security vulnerabilities. Among those surveyed, 85% cited the use of open source or commercial threat intelligence feeds, or a combination of both, within their current vulnerability management programs. Yet, how it is being used to score vulnerability risk is questionable. When asked how security vulnerabilities are prioritized today, 45% stated they are still using basic risk forecasting using the CVSS score and/or asset classification, or that correlation of threat intelligence and CVSS score was a manual process (see Figure 2).



The approach to information security overall is not keeping up with the pace of cybercriminals, and still remains very much a task driven by compliance compared to a core function for risk reduction. Two out of three (64%) respondents stated that compliance is still a key driver for how they approach information security programs such as vulnerability risk management. The existing view from the boardroom doesn't show much progress being made on this front, either. In fact, more than 60% of those surveyed stated company executives are only "somewhat" to "not at all" informed about the risk posed to their business from current day security threats.

Putting Management in Vulnerability Risk Management

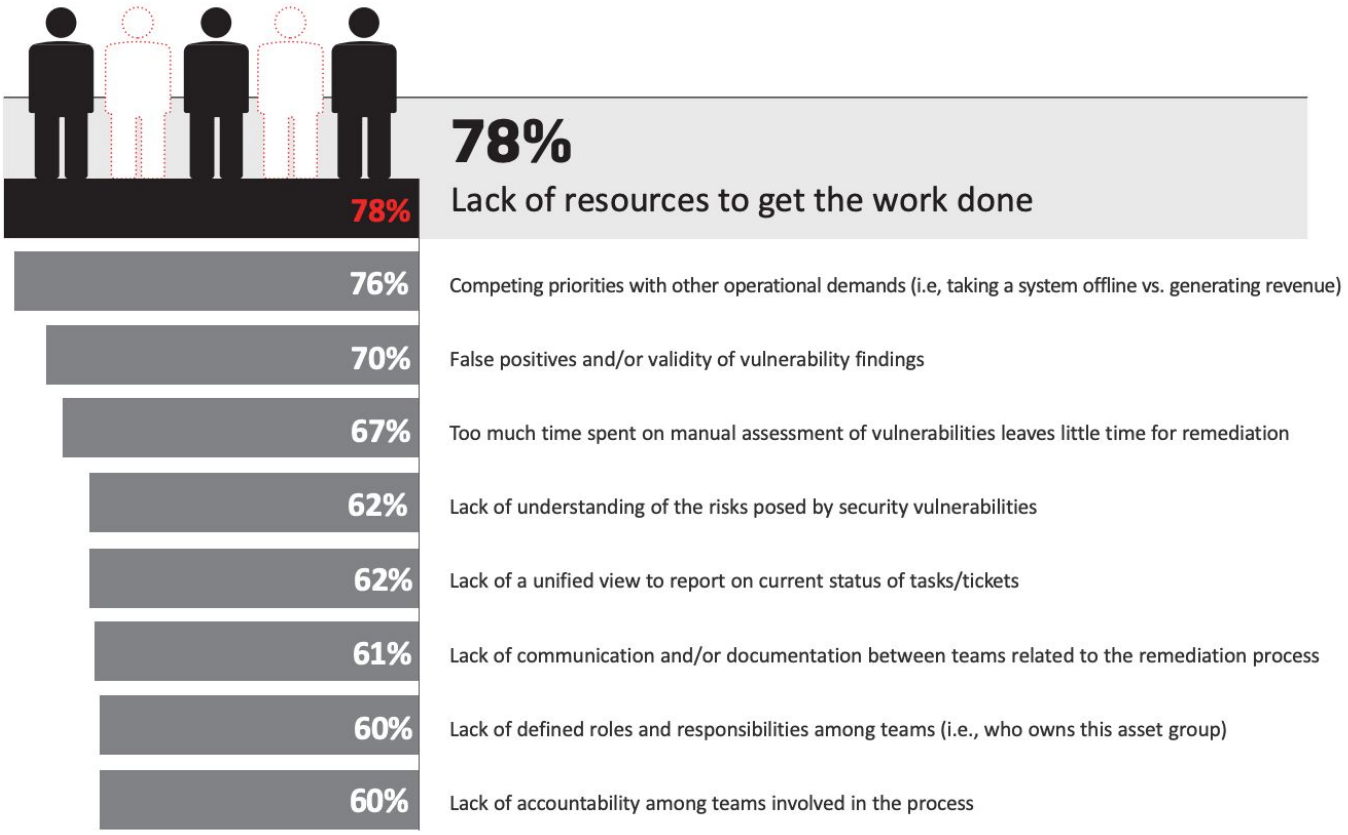
While lack of effective prioritization methods is certainly contributing to the lag time between detection and remediation of critical threats, the remediation process itself is riddled with gaps. On average, it takes 103 days for organizations to remediate a security vulnerability[4] . Even more, hackers are often staying inside the network for more than 200 days before they are detected[5] . This leaves the window of opportunity wide open for attackers and offers clear evidence that the remediation process is broken.

Respondents cited a very similar sentiment, with 82% stating their existing remediation process is broken, and 37% acknowledging "major improvement" is needed. There are many

[4] NopSec, "2015 State of Vulnerability Risk Management," June 2015
[5] FireEye, "M-Trends Report: A View from the Front Lines," February 2015

factors that are negatively impacting the current state of remediation, most notable being the lack of resources to get the work done (see Figure 3). Seventy-eight percent of those surveyed cited this as having the most impact, followed by competing priorities with other operational demands (76%) and too many false positives (70%).

Please rank how much each of the following challenges impacts the remediation process within your organization (percentages reflect organizations who indicated a moderate to major impact).



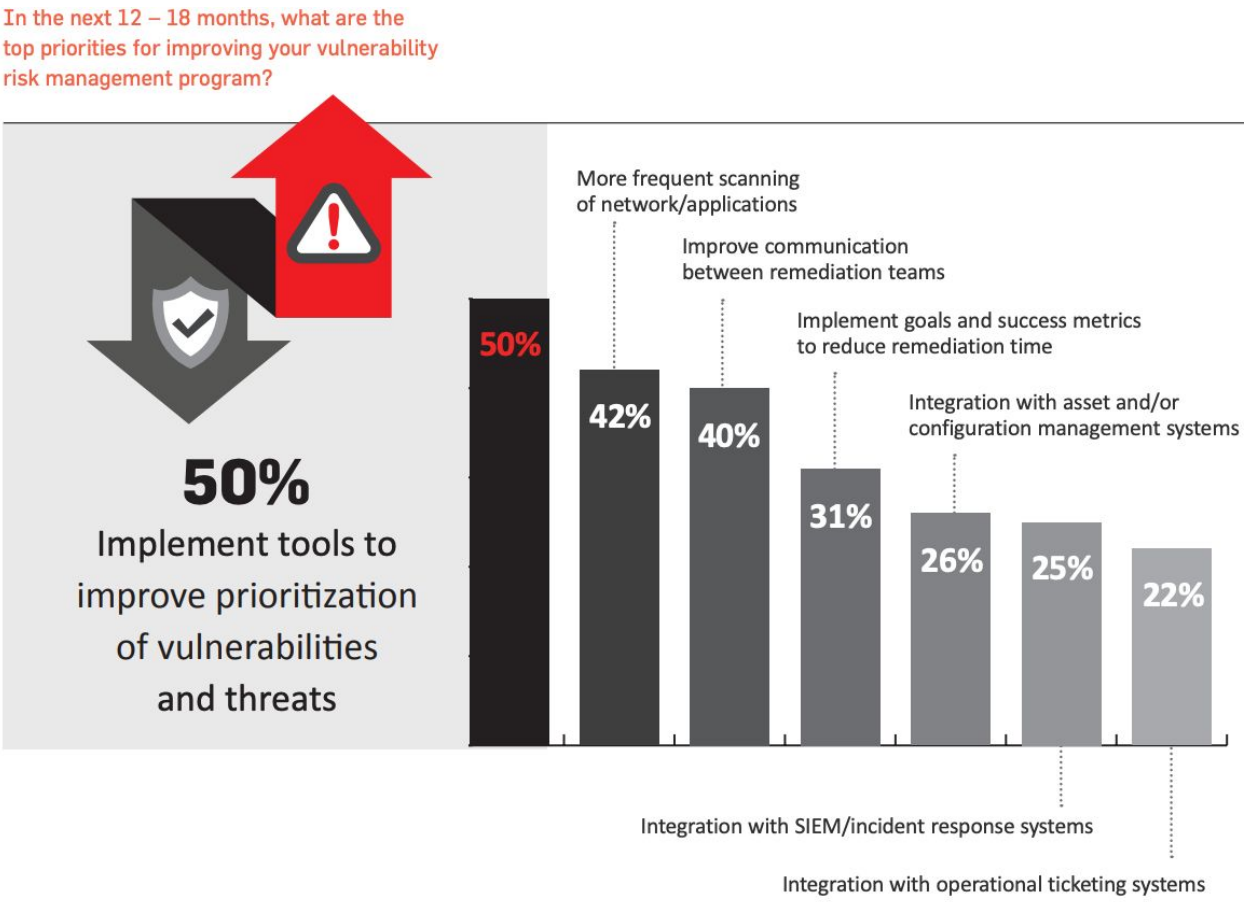
While technologies exist that can help improve the process through workflow automation and unified reporting, no program can be effectively managed if it can't be measured. This is especially true for teams involved in remediation where time is of the essence when it comes to fixing security vulnerabilities. For example, looking at hard metrics such as vulnerability aging can help internal teams identify the gaps and address them to

improve the process. Yet, only 40% of the organizations surveyed stated they have metrics in place to measure the success of their vulnerability management program.

2016 Outlook: Priorities in Vulnerability Risk Management

So much attention has been paid to anti-malware technology and incident response. As a result, many organizations have lost sight of the root cause to most data breaches – an exploited vulnerability. In examining many security incidents classified as an "advanced" attack, it is often nothing more than repackaged malware exploiting the same vulnerability over and over again. While an organization would never sit idle knowing an attacker is roaming their network, the same response does not hold true when it comes to vulnerability risk management. Breach after breach has shown through subsequent investigation that the headlines – and resulting costs and brand damage – could have been avoided by patching a single server or fixing a simple misconfiguration.

Organizations know improving prioritization and remediation is critical to drastically reducing the risk of a data breach, and were cited as top priorities in the coming year. Specifically, half of organizations surveyed plan to implement tools to improve the prioritization of vulnerabilities and threats, and 40% intend to work on improving communication between internal teams tasked with remediation (see Figure 4).



A recent report[6] of IT professionals showed that 59% say their companies don't invest enough in security. Despite increasing attacks and the recognized need for improvement in the coming year, it is unlikely security and IT teams will see increased budgets either. In fact, most forecasts have IT security spending as flat in 2016, which will be even more taxing on teams already faced with a lack of resources. The need for tools that enable automation of vulnerability risk management and other security processes to free up valuable resources will increase dramatically in the coming years as hackers continue to show no sign of slowing down.

[6] Spiceworks, "Voice of IT Report," October 2015

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.