4 Steps to Prove the Value of Your Vulnerability Management Program

Richard Kaufmann, CISO at Amedisys

“Within the healthcare vertical, my job as CISO isn’t to prevent a data breach.

My job is to increase the quality of patient care. The way that I do that is through reducing cyber threats, but at the end of the day, I’m here to make sure our patients get the right care, at the right place, at the right time.

My experience is that many security teams lose focus on that core mission that keeps their companies in business. When you aren’t part of the business plan, you are just another cost center.”

It's no secret that most cybersecurity teams are understaffed, underbudgeted, and underrecognized within their organizations: 60% of security professionals, to be exact, believe they are underfunded to carry out their jobs. However, building and delivering the right case to the executives and leaders who assess the "value" of your program could have game-changing downstream effects, such as the way your security operations are resourced and the perception of security as champions of the business, rather than blockers.

This eBook is designed to help you:

- Identify common pitfalls for measuring program effectiveness
- Deliver business-contextualized information to executives
- Understand if your current approach and technology support your overall goals

So you can:

- Prove the value and ROI of your vulnerability management program
- Be recognized and celebrated for your team's contribution to the business

Ready to bring new life to your program? Let's dive right in.

Move away from metrics that aren't impactful

For many years, the metrics we used to gauge the success of our vulnerability management operations were selected not-so-strategically, leveraging the information that was most readily available rather than what made sense for bigger-picture context.

Let's take a few examples:

Number of unpatched vulnerabilities or number of assets assessed

These numbers may sound important at first glance, but are of very little use to non-technical stakeholders like executives and board members; this is because they provide no link back to the priorities of the business, and are also not actionable.

CVSS score

While CVSS score can be a useful baseline metric to understand the nature of a vuln in isolation, it needs to be considered alongside metrics like malware exposure, exploit exposure, vulnerability age, and the importance of the asset to the organization. This added context helps you prioritize the risk most needing your attention. And, once again, CVSS score is unlikely to resonate with a non-technical audience.

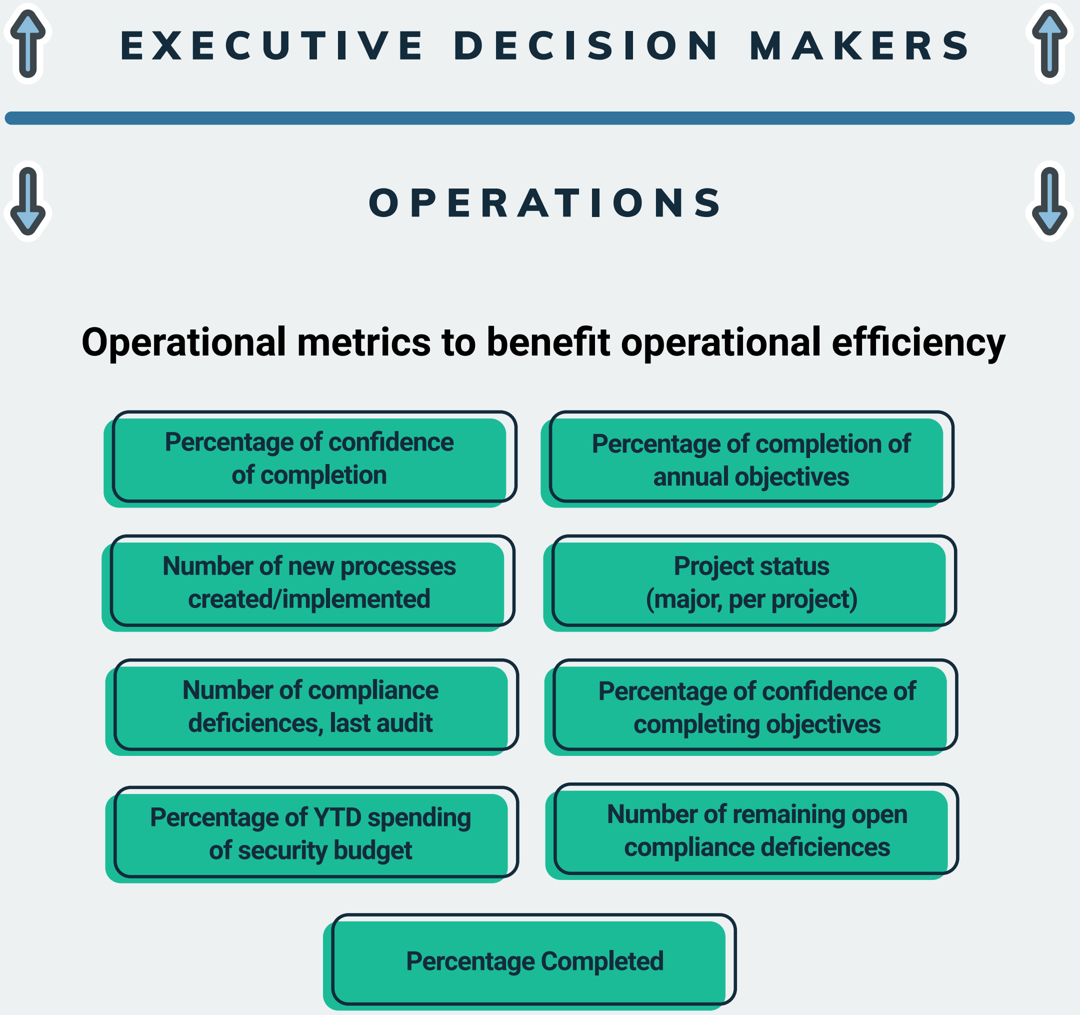
Metrics outside of your team's control, like aggregate risk score or number of cyber attacks

Wait... what? That's how I've been doing this for years. We know—but stick with us on this—what if right before you walk into a board meeting, there is a huge Patch Tuesday? Your aggregate risk score is going to spike, suggesting that your team has fallen down on the job, despite likely making progress since the last board meeting. Be cautious of these metrics, as you may be shooting yourself in the foot further down the line.

You might be feeling like you've been caught red-handed.

The good news? Operational metrics alone can't prove value or efficacy, but they can be building blocks for more meaningful analysis. The worst case scenario is that reporting on these metrics has limited your insight into your program, and painted the state of the program to be worse than it actually is; this leaves a near-term opportunity to positively change those perceptions (we're cautious optimists).

The even better news? We've already put some thought into how. We see a raise in your future.



EXECUTIVE DECISION MAKERS

OPERATIONS

Operational metrics to benefit operational efficiency

- Percentage of confidence of completion
- Percentage of completion of annual objectives
- Number of new processes created/implemented
- Project status (major, per project)
- Number of compliance deficiences, last audit
- Percentage of confidence of completing objectives
- Percentage of YTD spending of security budget
- Number of remaining open compliance deficiences
- Percentage Completed

Figure 1: Examples of operational metrics with limited impact "above the line" for Executive Decision Makers, per Gartner*

*Gartner, Develop Key Risk Indicators and Security Metrics That Influence Business Decision Making, Paul Proctor, Jeffrey Wheatman, Rob McMillan, Srinath Sampath, 31 July 2018.

STEP TWO

Adopt the metrics that matter

Before we get too far into the weeds, a brief primer on two distinct categories of metrics: Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs).
Did your eyes just glaze over? We promise to make this as painless as possible.

Key Risk Indicators (KRIs) are the operational metrics you are going to use to run your security program.

Key Performance Indicators (KPIs) are the metrics that the business uses to measure its effectiveness overall, with security and IT being one small (yet critical) piece of that overall picture.

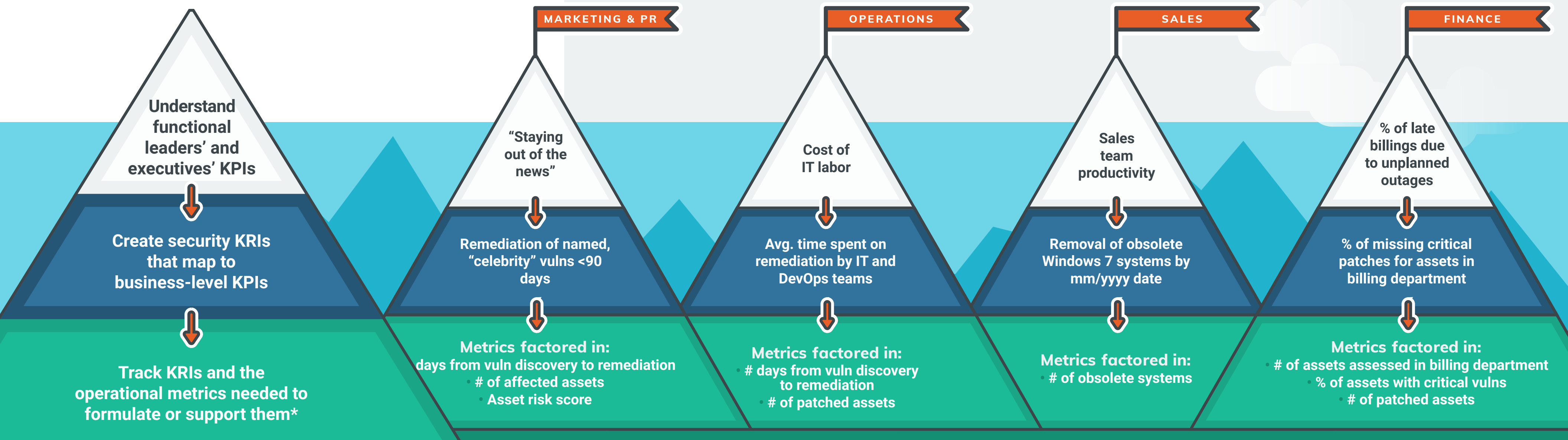
The key to presenting the right information to executive audiences is creating and aligning KRIs to business KPIs.

Asking yourself, ***"Where am I even supposed to find my company's KPIs?"*** One place to start is with the heads of each functional group in your organization. In simplest form, you can initiate conversations around their current pain points and priorities, and what types of improvements they're working towards. From there, you can continue to prioritize functional needs based on the company's yearly goals (perhaps even a "three year plan") or timely response to an external event, for example.

By taking a KPI business metric and creating a KRI equivalent, it can be understood by all other non-technical counterparts, relay the importance of security to the business as a whole, and garner better relationships, trust, and budget. Good KRIs establish clear, causal relationships to business outcomes, and address their target audience without excessive jargon and operational details.

For instance, if your organization has a sales team, there is undoubtedly a KPI measuring their productivity. As a security team, you've observed that employees are more productive with up-to-date operating systems (e.g. fewer system malfunctions, enhanced functionalities, etc.). By establishing this link through a KRI, you can communicate your team's value with statements such as,

"We've helped the organization achieve its goal of increasing sales team productivity 5% this quarter by progressing towards our security team goal of removing all Windows 7 workstations by the end of Q1 2020."



Understand functional leaders' and executives' KPIs

Create security KRIs that map to business-level KPIs

Track KRIs and the operational metrics needed to formulate or support them*

MARKETING & PR

"Staying out of the news"

Remediation of named, "celebrity" vulns <90 days

Metrics factored in:
- days from vuln discovery to remediation
- # of affected assets
- Asset risk score

OPERATIONS

Cost of IT labor

Avg. time spent on remediation by IT and DevOps teams

Metrics factored in:
- # days from vuln discovery to remediation
- # of patched assets

SALES

Sales team productivity

Removal of obsolete Windows 7 systems by mm/yyyy date

Metrics factored in:
- # of obsolete systems

FINANCE

% of late billings due to unplanned outages

% of missing critical patches for assets in billing department

Metrics factored in:
- # of assets assessed in billing department
- % of assets with critical vulns
- # of patched assets

Figure 2: How to Create Key Risk Indicators (KRIs): A step-by-step process

STEP THREE

Create goals and a sustainable reporting process

Now that you've exercised how to map security KRIs to business KPIs, it's crucial to solidify these KRIs as the goals and service level agreements (SLAs) you and your team are accountable for. This framework isn't designed to add responsibility to your plate—rather, it's setting you up for longer term success.

Establishing goals and SLAs will:

- Anchor your team's efforts (think of them as a "north star").
- Provide you with the primary reference point for presenting to non-technical stakeholders.

With goals and SLAs now aligned to the most pressing needs of the business, you can better illustrate how security is essential to keeping things in operation. You'll also be met with less resistance asking for resources and support needed to achieve those goals.

One example is a service level commitment like, **"80% of critical vulnerabilities will be patched on payroll-related systems within 7 days."** This kind of KRI exhibits how you're protecting the business' most important systems and data.

> **"In Q3 2019 we achieved our SLA for critical patched on payroll systems 70% of the time."**

> **"Because of increased investment and team training, we achieved a 95% adherence to this SLA in Q4 2019."**

With this approach, you can acknowledge your team's progress, make a compelling case for additional support, and open the door for more productive conversation.

The delivery, however, can be just as critical to securing a positive outcome. You guessed it: Let's talk reporting.

So, what makes for an effective report?

By nailing down your reporting process to deliver the right information to the right audience at the right time, you can properly highlight your team's wins and gain buy-in at the executive level.

We're officially in the home stretch.

WHAT TO LOOK FOR	WHAT TO WATCH OUT FOR
Simple and scannable graphs and summaries of pertinent data	Graphs and charts presented with little context
Visualization of how you're trending over time	Reports that are snapshots-in-time
Inclusion of data that is actionable and within your team's control	Reports that include metrics uncontrollable or unchangeable by your internal security team
Reporting frameworks and templates that can be tailored to different audiences	Generic reporting templates that cannot be customized or that take significant, manual effort to customize

STEP FOUR

Invest in technology that supports your program goals

While we've had plenty of time to discuss revamping your approach to proving value, it's time we address where the boots meet the ground.

Without the right technology supporting your program, it will be significantly more laborious to first get the information you need when you need it, then deliver that information quickly and concisely. That's why we've put together a handy checklist of capabilities a vulnerability risk management solution should possess to facilitate your vendor evaluation.

Does your current vulnerability risk management solution enable you to:

- ✓ Easily find and organize data to align with the priorities of your program?
- ✓ Track and measure the goals and service level agreements (SLAs) most pertinent to your program?
- ✓ Visualize progress towards those goals and SLAs over time?
- ✓ Create customized reports and dashboards for various stakeholders?

While these aren't necessarily non-negotiables, they do significantly reduce manual effort required on your end that you could be re-allocating towards more strategic initiatives or team training. Not to mention, a solution designed with these workflows in mind will reduce the learning curve of adopting this new approach and mindset.

With this final step in place, you can reach new heights in the way you and your stakeholders view, assess, and ultimately respect your vulnerability management program.

LEARN MORE

And now, a brief message from, well, us:

Rapid7 InsightVM, our leading vulnerability risk management solution, is designed to help teams like yours achieve. That means saving you time and effort on traditionally manual and tedious processes, visualizing how your program has progressed over time, and facilitating communication with leadership in ways that resonate and recognize your accomplishments.

To learn more about how InsightVM capabilities like Live Dashboards, Remediation Projects, and Goals and SLAs can help you do exactly that, visit us at [www.rapid7.com/insightvm.](http://www.rapid7.com/insightvm)

About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Customers around the globe rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. To learn more about Rapid7 or get involved in our threat research, www.rapid7.com.