PROVING PERFORMANCE:
USING METRICS TO BUILD A STRONG CASE FOR APPLICATION SECURITY

Achieving support and securing resources for your application security program requires facts, numbers and proof points.

VERACODE

INTRODUCTION

Today, enterprise leaders are painfully aware that cybersecurity risks exist. The frequency and intensity of attacks continues to trend upward, and a growing number of organizations find themselves targets of hackers, attackers and cyberthieves. **In Q3 2017, according to a 2017 report by Akamai, there was a 30% increase in web application attacks compared to Q2 2017.**[1] And according to the 2018 Cyberthreat Defense Report, 77% of organizations have been victimized by one or more successful cyber attacks - which is an increase of 15% since 2014.

TWEET THIS

Despite the prevalence of attacks, achieving buy-in to build and grow a strategic framework that protects data, assets and intellectual property is fraught with challenges. Where many organizations fall short is in assembling a business case that supports targeted investments and resources. Without a focus on core metrics, key performance indicators (KPIs) and other data that clearly demonstrate the benefits of deploying specific tools and technologies, it's impossible to put resources to work effectively.

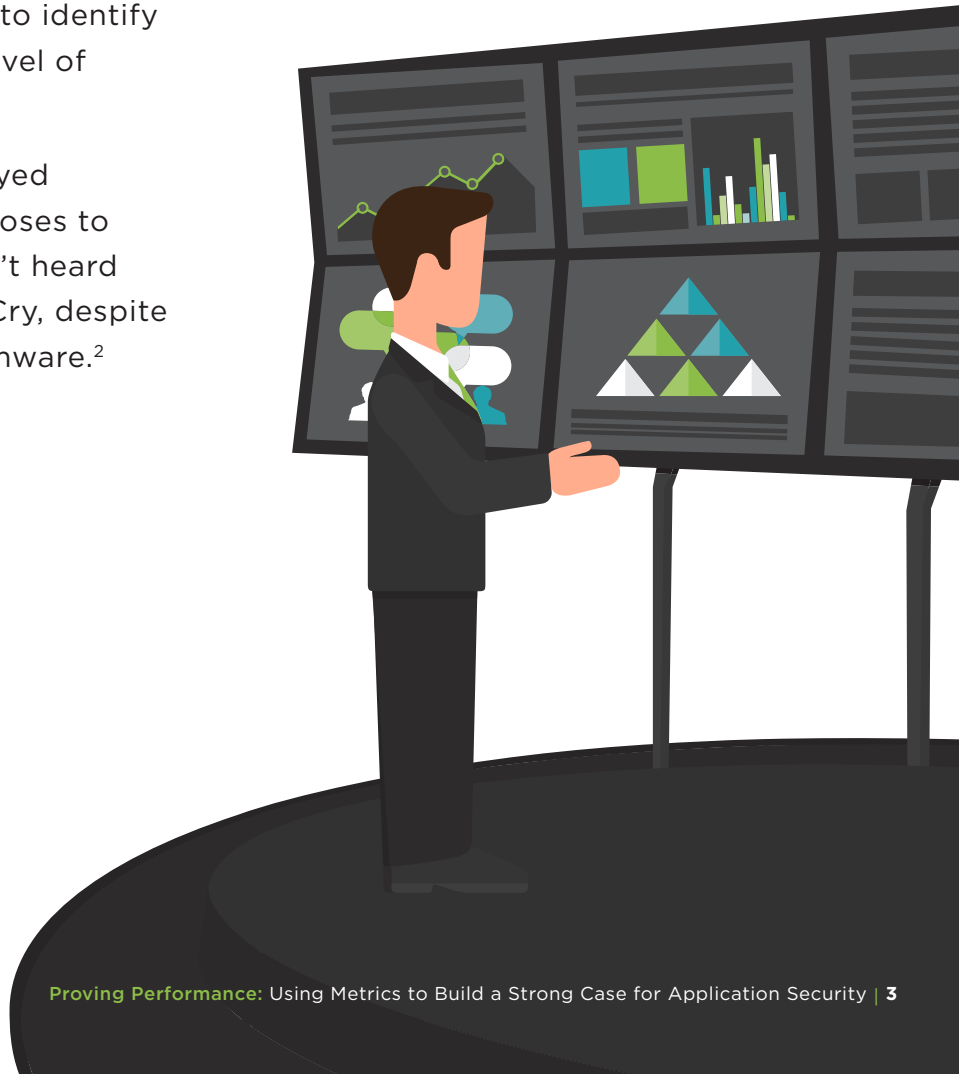
On the other hand, when those who head an application security initiative build a business case with the use of key metrics, the end result is typically lower costs, improved protection, real world gains in security and proof that you're removing risks from the organization — proof that can help you get the buy-in you need to expand your efforts.

WITHOUT A FOCUS ON METRICS, KEY PERFORMANCE INDICATORS (KPIS) AND OTHER DATA THAT CLEARLY DEMONSTRATE THE BENEFITS OF DEPLOYING SPECIFIC TOOLS AND TECHNOLOGIES, AN ENTERPRISE WILL LIKELY FIND ITSELF AT RISK — OR, WORSE, THE VICTIM OF A SERIOUS BREACH OR BREAKDOWN.

THE CASE FOR APPLICATION SECURITY

Because application security touches various departments and functions, there's a need for support and buy-in across the organization. For organizations starting from ground zero, it's critical to build a case for an application security program. For those with an existing framework, it's vital to gain or solidify support in order to expand or broaden your application security initiative. Frequently, organizations that stumble or fail in the cybersecurity arena make decisions blindly. They're unable to identify key factors that drive results, and they often lack the necessary level of communication to achieve support from the executive suite.

A recent Veracode survey found that only about half of the surveyed business leaders recognize the full risk that vulnerable software poses to their enterprise. In addition, the vast majority of executives haven't heard of specific threats, such as Heartbleed, Struts-Shock, and WannaCry, despite a string of high-profile attacks and growing problems with ransomware.[2]



WITHOUT CLEAR APPLICATION SECURITY MEASUREMENTS OR METRICS IN PLACE, AN ENTERPRISE IS ESSENTIALLY FLYING BLIND AND SUBJECT TO DECISIONS BASED ON HUNCHES AND OPINIONS RATHER THAN FACTS AND LOGIC. THIS ISN'T A FORMULA FOR LONG-TERM SUCCESS IN THE CYBERSECURITY SPACE.

Unfortunately, without clear goals with measurements or metrics in place, an enterprise is essentially flying blind and subject to decisions based on hunches and opinions rather than facts and logic. It's also mired in a reactive mode that involves taking action only after a problem or breach occurs. This isn't a formula for long-term success in the cybersecurity space.

Not surprisingly, an organization that adopts this approach usually winds up with misaligned or unaligned tools, incentives and results. It spends money and uses cybersecurity resources inefficiently — while falling short of the level of protection required for today's world. What's more, new or additional resources are difficult to obtain because the senior leadership team doesn't recognize a need. However, even organizations with a set of metrics can stumble. With the wrong measures in place, leaders may believe the organization is secure because it is hitting all of its metrics. Yet, critical concerns may fly below the radar and the enterprise may, in the end, wind up with a nasty shock in the form of a hack or intrusion.

Yet, real-world application security benefits exist and they are measurable. A recent CA Technologies survey found that those organizations with mature software security programs that embed security testing into development processes were:

- 2.4 times more likely to be leveraging security to enable new business opportunities
- 2.5 times more likely to be outpacing their competitors
- Have 50 percent higher profit growth and 40 percent higher revenue growth[3]

By using metrics and tangible data to support an application security initiative, you can take performance to a higher level and demonstrate that you are guiding the enterprise to a safer and better place.

MAKING METRICS MATTER

Developing a core set of metrics presents a few challenges. For one thing, every industry and business is different — and internal needs evolve over time. For another, different departments and groups in the same organization may require different metrics and KPIs to fulfill their mission. For example, a chief information security officer (CISO) might examine how many web applications the organization is scanning at any given moment; developers might focus on how many software applications require a fix; and senior executives might focus on cost savings and definable risk reduction.

Because there's no template or set list of metrics, every organization must approach application security differently. It's critical to identify and understand the specific factors that impact your enterprise and the groups within it. This may include things such as how many applications meet internal security policies, how frequently an organization is testing and retesting them for vulnerabilities, and the scope and types of risks present and how they map to real-world costs, particularly if a breakdown occurs.

Typically, metrics revolve around four core areas:

1. Policy compliance.

It's crucial to identify an acceptable level of risk for any application that your organization places into production. Without policy-based metrics, there's no way to gauge performance or progress. This process involves benchmarking where your organization stands when it begins an application security initiative — typically focusing on the OWASP Top 10 (which encompasses the top 10 vulnerability categories). Veracode recently found that the pass rate for OWASP Top 10 compliance among its customer base was only 22.5%.[4]

2. Flaw prevalence.

This metric spotlights how common a risk is within a particular industry or business. It helps an organization prioritize threats such as SQL injection, Cross-Site Scripting (XSS), cryptographic issues and CRLF injection based on real-world impact.

3. Fix rate.

Effective application security is about more than finding flaws; it's about fixing them. You aren't measuring the true progress of your program if you aren't monitoring your fix rate. And if it's not where it should be? Developer knowledge might be to blame. Most developers have not had security training. **Veracode research has found that eLearning improved developer fix rates by 19%; remediation coaching improved fix rates by 88%.**

TWEET THIS

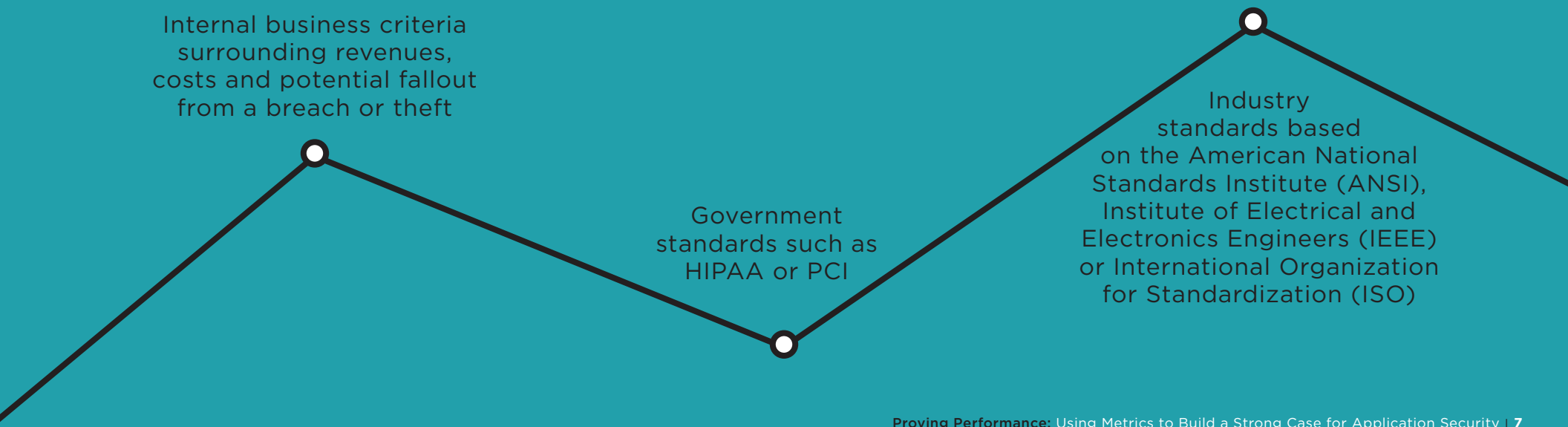
4. Business- and goal-specific metrics.

These criteria are dependent on organizational goals and objectives. As a result, they vary across organizations. For instance, a core metric may touch on developer education or the number of applications that have been assessed or retired. It might also include the percentage of applications where testing has been fully integrated.

Once an organization has identified the key issues in application security that matter most, it can adjust the levers to fit the specific circumstances. It can also build a set of aggregate metrics and sub-metrics that, while tightly revolving around policies, are flexible enough to fit the needs of different groups and departments. Typically, between three and a dozen metrics are necessary. However, an organization might also layer metrics so it's possible to view an initial set through a dashboard or reporting functions and drill down through layers to gain additional perspective, based on unit or departmental requirements.

It's also critical to distinguish between leading indicators and success metrics when developing a set of criteria. The former represents high-level insights that guide the organization and the latter are often the nuts and bolts of an initiative. For example, within an internal development program, a leading indicator may be the number of applications the organization is scanning, while the success metric addresses the number of applications that adhere to policy and the percentage of vulnerabilities that have been found and fixed. For an externally developed application program, a leading indicator may be how many vendors are on board with the application security program, while the success metric is the percentage of policy violations in the code.

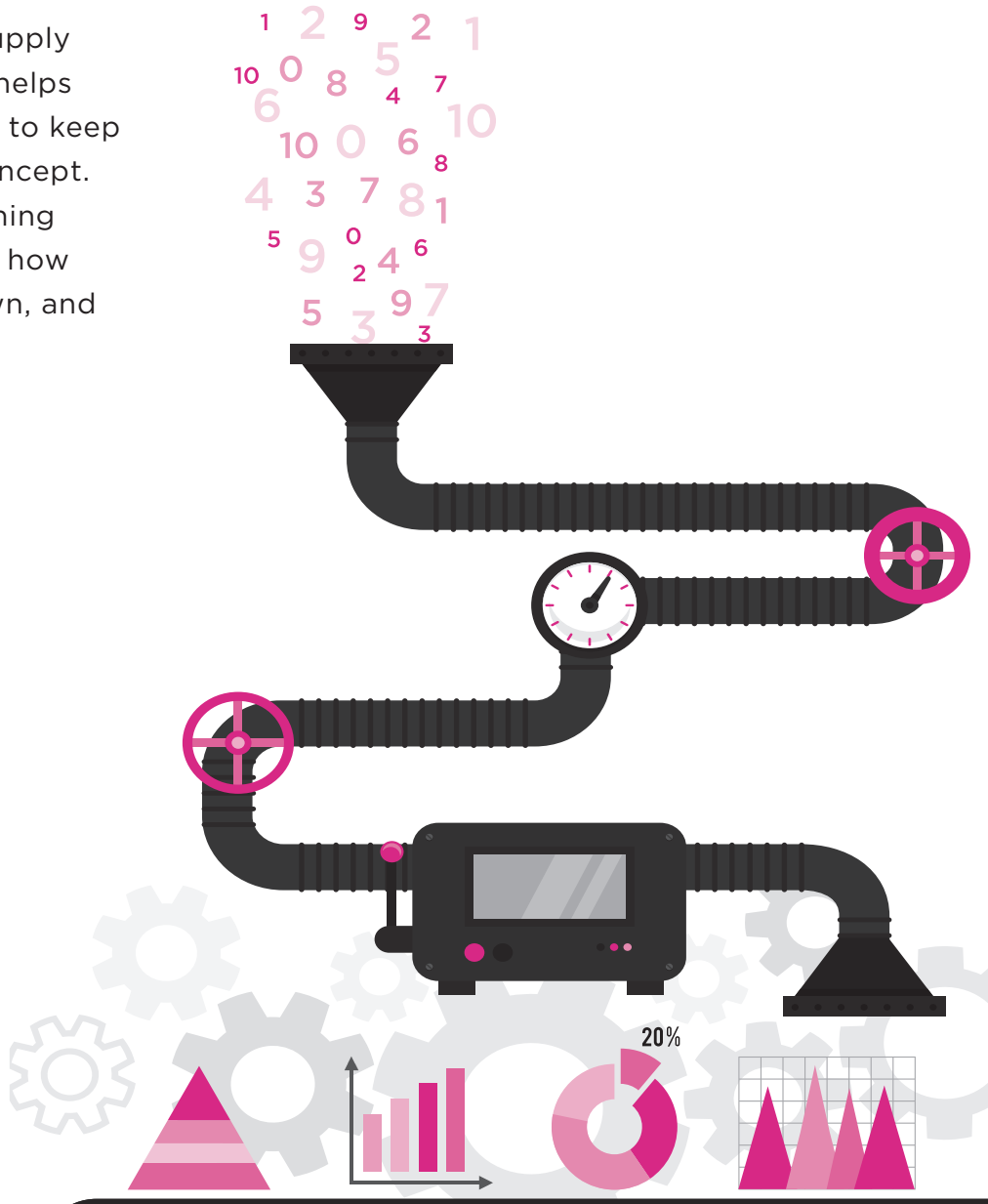
Key sources for developing and validating metrics may include:



BY THE NUMBERS

A best practice approach requires an IT framework that can supply accurate data for metrics — including a scanning service that helps identify and remediate vulnerabilities. Moreover, it's important to keep groups informed and continually sell the importance of the concept. This means, among other things, providing education and training so employees and others can understand metrics, recognizing how and why they're important to departments other than their own, and understanding how to make key decisions based on data. It's also wise to promote an initiative beyond the initial planning and implementation process. An internal marketing team should publicize results and wins as they unfold.

Likewise, whether you're launching an application security program or looking to persuade enterprise leaders to expand an existing program, it's important that executives in the C-suite understand the importance of metrics and results so your organization can adopt a fact-based approach. Unfortunately, many CSOs and CISOs continue to justify additional spending in order to ensure that "nothing" continues to happen. Yet when enterprise leaders view easy-to-digest metrics, and these metrics and KPIs map to definable actions, a strategic approach follows and the necessary investments and steps for application security become clear. Combined with the right technology tools, peer mapping, audit and compliance tracking, and communication and collaboration systems, it's possible to keep everyone in sync — and an enterprise more secure.



5 Best Practices for Putting Metrics to Work

1. Start with the assumption that executives and other employees have a minimal understanding of security metrics and how to apply them.

2. Identify key metrics that drive results in your industry and business. This requires input from different business leaders within the organization — usually with the CSO or CSIO overseeing the process.

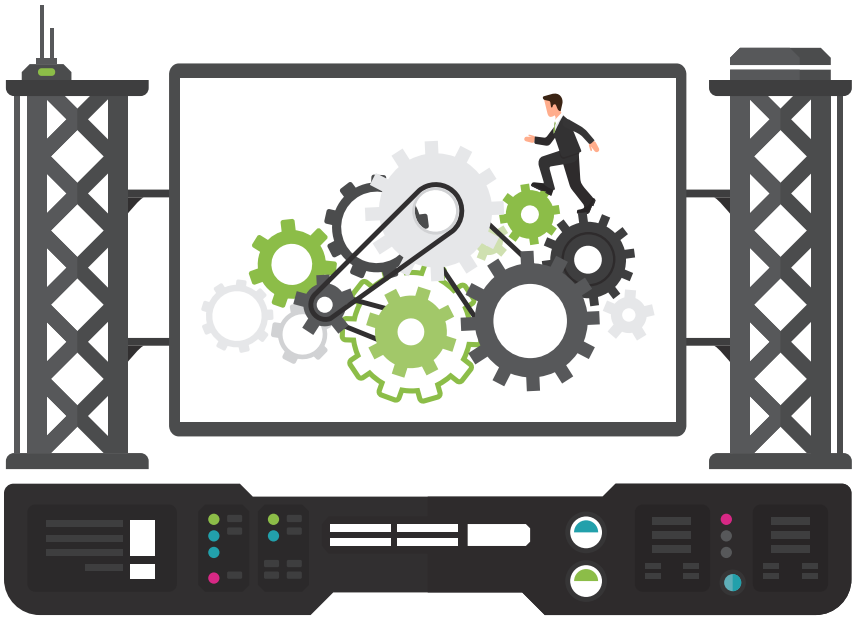
3. Take a cross-functional and interdepartmental approach in order to identify core issues, develop a strategy and a tactical plan, and put the plan into action.

4. Provide classroom instruction and/or training sessions to help everyone get up to speed.

5. Reevaluate key metrics periodically.

CONCLUSION

When an organization adopts a cybersecurity strategy that revolves around data and metrics, it's possible to move beyond a reactive and ad hoc approach to cybersecurity and adopt a proactive model. This will help your organization allocate application security resources, including investments, in an optimal manner as well as help you achieve the buy-in and support you need to grow your program to better protect your enterprise. This can help you and your organization achieve maximum return on investment and greatly reduce the risk of a breach.



LEARN MORE

Are you looking to transform your application security program into a strategic success? Learn more about metrics and what goes into building a strong application security framework by listening to this webinar from Veracode, **The Fantastic Four: Metrics You Can't Ignore When Reducing Application-Layer Risk**.

WANT TO SEE HOW YOU MEASURE UP WITH APPLICATION SECURITY?

Get all the latest news, tips and articles delivered right to your inbox by subscribing to our blog.

www.veracode.com/blog

ABOUT VERACODE

Veracode's cloud-based service and systematic approach deliver a simpler and more scalable solution for reducing global application-layer risk across web, mobile, and third-party applications. Recognized as a Gartner Magic Quadrant Leader since 2010, Veracode secures hundreds of the world's largest global enterprises, including three of the top four banks in the Fortune 100 and 20+ of Forbes' 100 Most Valuable Brands.

LEARN MORE AT WWW.VERACODE.COM, ON THE VERACODE BLOG, AND ON TWITTER.

VERACODE

---

1. *Q3 2017 State of the Internet / Security Report*, Akamai.
2. *Securing the Digital Economy*, Veracode.
3. "Integrating Security into the DNA of Your Software Lifecycle," CA.
4. *The State of Software Security, Volume 9*, Veracode, 2018.