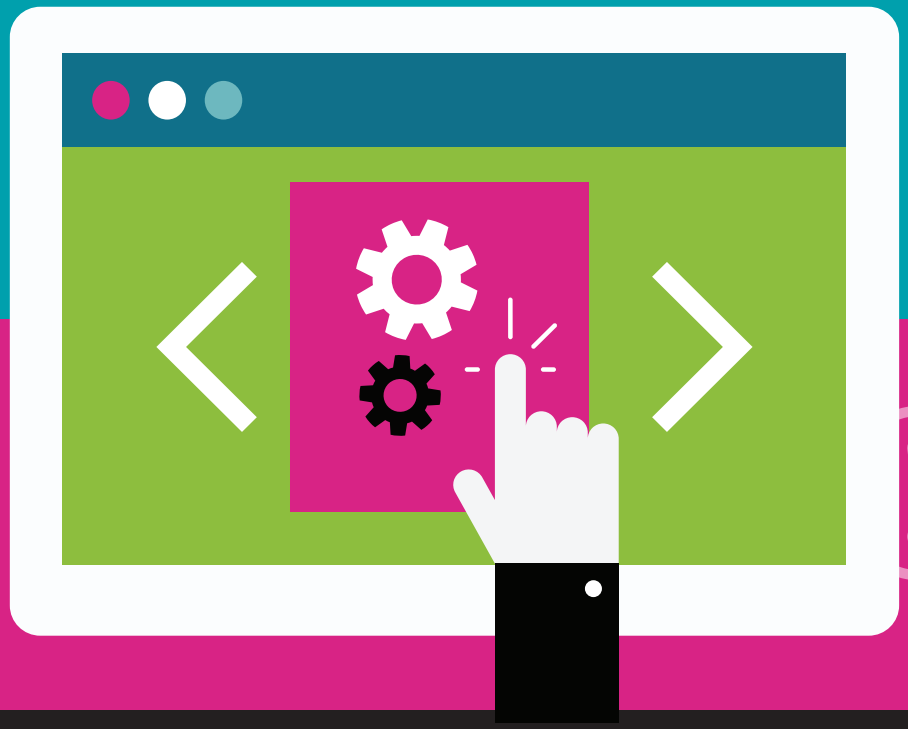
POLICY POINTERS:

A BEST-PRACTICE APPROACH TO APPLICATION SECURITY GOVERNANCE

A well-conceived framework of application security policies boosts protection and lowers costs.



VERACODE

A NEW ERA EMERGES

Today's cybersecurity landscape is nothing less than ominous. Collectively, organizations spend somewhere in the neighborhood of $75 billion annually for an array of tools, technologies and solutions.[1] Enterprise security specialists devote countless hours to stamping out a seemingly endless stream of threats.

Yet, as organizations accumulate an expanding mountain of internal code, as well as third-party applications, there's a growing awareness that application security is often at the center of an effective security strategy. This, too, presents significant challenges. Scanning code for vulnerabilities represents only part of the solution. There's a need to introduce a strong governance framework with a set of policies that increases protection and decreases risk.

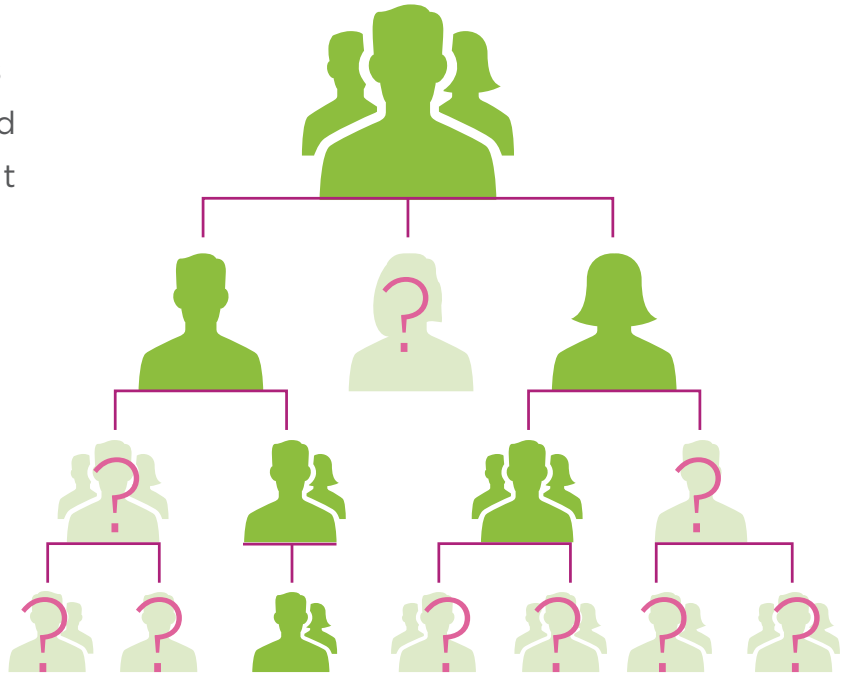
FACT

Attacks on the application layer are growing at a rate of about **25% per year.**[2]

BEST PRACTICES ARE ALL ABOUT DOLLARS AND SENSE

A strong application security framework boosts an organization's ability to manage growing and often vast libraries of software and code. While there's no single path to success, it's important to put a set of best practices into play.

This governance framework can go a long way toward creating a uniform and consistent approach across the enterprise — and even out to partners and others. It helps an organization enforce security policies across all applications and portfolios. It also increases the odds that an enterprise adheres to regulatory compliance requirements, as well as industry standards, and that teams are working in a consistent and synchronized way.



FACT

There are currently **more than 209,000 unfilled cybersecurity jobs** in the U.S.[3]

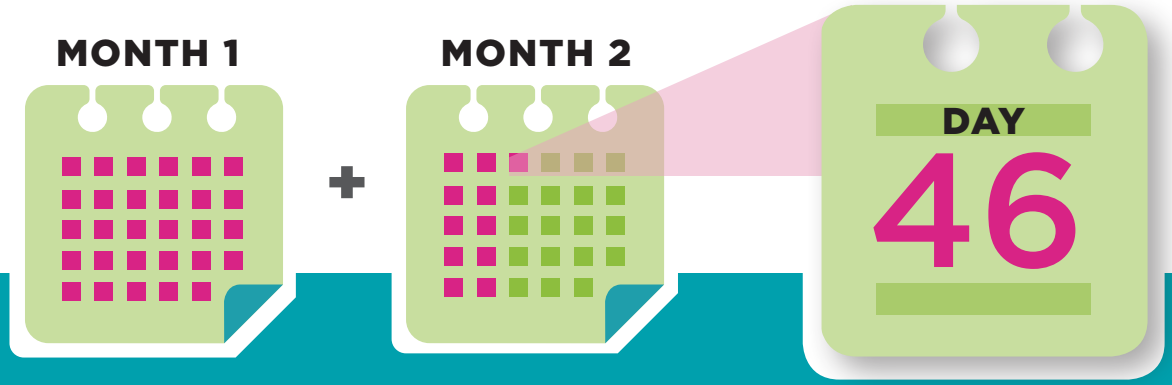
PUTTING BEST PRACTICES TO WORK

Here are 8 ways to keep your organization on track in the application security arena:

BEST PRACTICE #1:

Adopt a cross-functional approach to policy building.

Poorly constructed policies lead to poor results. They also lead to violations — not because development teams and others are looking to do harm, but because they may ignore or minimize risks along the way. The key to matching policies with practical requirements? Understand business and security requirements from different groups, including line of business, the legal department, procurement staff and developers.



FACT

The mean number of days to resolve cyberattacks is **46,** with an average cost of **$21,155 per day** — or a total cost of **$973,130** over the 46-day remediation period.[4]

BEST PRACTICE #2:

Create policies based on both internal and external challenges.

Internal and external application security requirements aren't created equal. Attempting to enforce policies that don't match business, security and software needs often leads to misalignment — and increased vulnerabilities. Ultimately, policies must be flexible enough to accommodate these outside players, while ensuring that internal systems remain protected. Key factors include: use case, type of application, risk profile, compliance requirements and auditing needs.

FACT

Average annual cybercrime losses to companies worldwide now exceed **$7.7 million.**[5]

BEST PRACTICE #3:

Focus on security rather than program participation.

It's incredibly easy to set the bar too high. While a high standard of security is vital, unrealistic expectations and requirements too often lead to people looking for ways to get around policies so they can get their work done. A basic fact of application security is that any policy should be only as complicated as it needs to be to deliver the necessary results. A more realistic approach starts with attainable goals — such as the eradication of a specific high-risk threat — and expands from there.

FACT

Enterprise security governance practices moderate the cost of cybercrime. Companies that employ expert staff can reduce cybercrime costs by an average of **$1.5 million.**[6]

BEST PRACTICE #4:

Use industry standards as a barometer.

It's important to establish a barometer — and a starting point — for building application security policies. Industry standard lists, such as the OWASP Top 10 or SANS 25, can help track threats that are relevant to a business or industry. For example, a business might set a goal to completely eliminate a particular risk that matches common industry criteria or to tie findings to a compliance standard, such as PCI or HIPAA. An organization might also evaluate apps and coding practices based on risks, or on auditing considerations.

FACT

A recent analysis found that components introduce an average of **24 known vulnerabilities into each application**.[7]

BEST PRACTICE #5:

Address vulnerabilities rather than flaws.

While it's important to identify flaws that may fall into the OWASP Top 10 or the CWE/SANS Top 25, it's even more important to distinguish between flaws that represent a remote risk and those that represent more substantial, real-world risks. In some cases, the likelihood of a vulnerability being exploited may be low, but the potential damage might be great. In other instances, the chance of exploit might be high, but the damage may not be substantial.

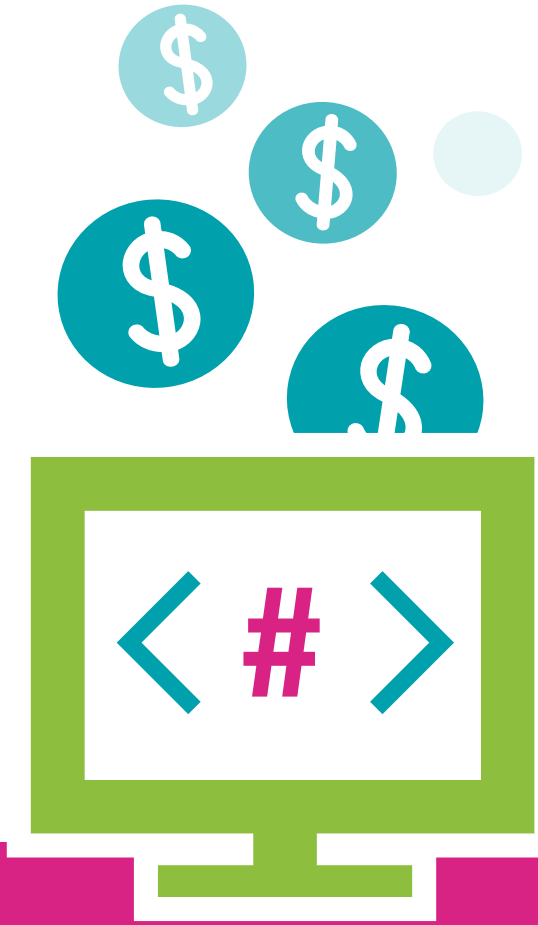
FACT

74% of enterprise security executives **expect a cyberattack in 2016**.[8]

BEST PRACTICE #6:

Weigh remediation versus mitigation.

No organization has unlimited money and resources to address cybersecurity risks. Simply handing development teams a tool and asking them to translate the findings into fixes is likely to result in high costs and ineffective protection. The objective isn't to perform triage on what the tool reveals and wind up chasing down every vulnerability — it's to fix what really needs to be fixed, particularly as multiple departments and shared business outcomes enter the picture.



FACT

60% of enterprise information security budgets will be allocated to rapid detection and response approaches by 2020 — up from less than 10% in 2014.[9]

BEST PRACTICE #7:

Measure results.

Gauging performance and results is critical. Metrics and key performance indicators (KPIs) can help an enterprise understand compliance, flaw prevalence, fix rates and business- and goal-specific performance. They provide insight into various factors, such as how many applications meet internal security policies, overall flaw density, how frequently an organization is testing and retesting apps for vulnerabilities, the scope and types of risks present, and how they map to real-world costs.

FACT

Organizations that deploy an effective application security solution framework **reduce vulnerabilities by 60%.**[10]

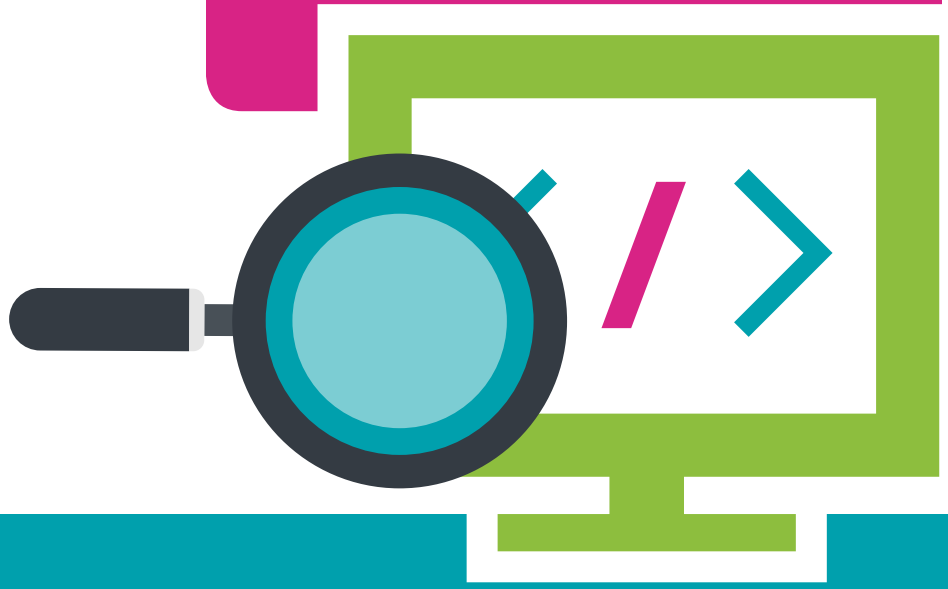
BEST PRACTICE #8:

Update policies as necessary.

The cybersecurity landscape is in constant motion. New threats and vulnerabilities are a constant concern. In addition, organizational needs may change, based on new and different partnerships, third-party software, open-source platforms and emerging technologies. The takeaway? It's critical to update policies on a regular basis. An organization's ability to build a strong, yet flexible, policy framework goes a long way toward defining its success in the application security arena and beyond.

FACT

50% of global 500 organizations **use open-source code with known vulnerabilities**.[11]



APPLICATION SECURITY IS A MATTER OF POLICY

As pressure mounts to produce applications faster and incorporate third-party software, open-source code and APIs, a strong application security framework is paramount. Yet even the best scanning tools are ineffective without a robust set of policies. An organization may wind up focused on the wrong risks or sink under the weight of test results that cannot be prioritized. An application security program with a strong governance framework helps teams work faster and better. It helps an organization achieve the best possible protection.

REFERENCES

[1] "Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015," Gartner. September 23, 2015.

[2] Akamai Releases *Q3 2015 State of The Internet - Security Report*, Akamai, December 8, 2015.

[3] "Demand to Fill Cybersecurity Jobs Booming," Peninsula Press. March 31, 2015.

[4] *2015 Cost of Cyber Crime Study: Global, Ponemon Institute*, Hewlett-Packard Enterprise, October 2015.

[5] Ibid.

[6] Ibid.

[7] "Open Source and Third-Party Components Embed 24 Known Vulnerabilities into Every Web Application on Average," Veracode. October 22, 2014.

[8] *State of Cybersecurity, Implications for 2016: An ISACA and RSA Conference Survey.*

[9] Ibid.

[10] *The Total Economic Impact of Veracode's Cloud-Based Application Security Service,* Forrester Research (sponsored by Veracode), July 2014.

[11] *SANS Survey on Application Security Programs and Practices*, SANS Institute, December, 2012.

For more details on creating effective application security policies for your organization, see our guide, *Policy Matters: How to Build a Robust Application Security Governance Framework.*

VERACODE