EVERYTHING YOU NEED TO KNOW ABOUT

GETTING APPLICATION SECURITY BUY-IN

VERACODE

Application security is unlike other forms of security in that it directly impacts the daily routines of your co-workers. When you implement new anti-virus software, most employees won't notice, and when you create a new firewall rule, it generally doesn't impact anyone except the network manager creating the rule.

But application security is different. First, it requires the participation of the development team and has the potential to disrupt their software development lifecycle — which in turn negatively impacts their ability to meet production schedules. And it isn't just development teams that are impacted. The consumerization of IT means employees in all departments are purchasing and downloading software. If your program includes a security-vetting process for the purchase of third-party software (as it should), then you're slowing these employees down as well. Or worse, your policy may prohibit them from purchasing software that helps them do their job.

Even the most well-thought-out plan, with strong policies, guides and metrics, will fail if those policies aren't followed. The simplest way to ensure your policies are ignored and your efforts at reducing risk are in vain is to create your program in a silo.

Application security cannot take place in a vacuum. Its impact on multiple groups in an organization makes it necessary to work with, and gain buy-in from, groups such as:

- Development teams
- C-suite
- Legal team
- Procurement organization
- Marketing

DOWNLOAD

Joining Forces: Why Your Application Security Initiative Needs Stakeholder Buy-In explains why it's essential to get buy-in for your AppSec program from key departments in your organization, and discusses the roles these departments will play in the success of your initiative.

EXECUTIVE BOARD/C-SUITE

WHY YOU NEED EXECUTIVE BUY-IN

The board of directors, the C-suite, and the other members of your executive team — including the chief information security officer (CISO) — play a central role in supporting and sponsoring application security. They're integral to strategic alignment, sponsorship across the organization, delivering essential financial and human resources, and supporting a framework for collaboration and communication.

Sponsoring

If you have support for your application security program from the executive team, other departments in the organization will be compelled to participate and support the program as well. If affected departments don't understand and embrace the changes brought about by your program, you're stalled.

Scaling

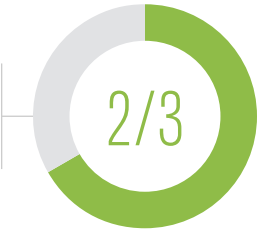
Ultimately, the more support the application security program has from the C-suite, the more likely the security team will be able to scale the program to cover the entire application layer over time. The end goal needs to be a mature, robust application security program that secures every application at your organization, regardless of origin. It's not enough to secure only the applications you build or only the business-critical ones. Recent high-profile and costly breaches have stemmed from non-business-critical third-party applications and open source components. Your organization isn't truly secure unless your application security program can assess every application, with the ability to scale as your organization expands and changes.

Getting buy-in for pen testing a few apps but not creating a comprehensive program? Get tips on making the case for an AppSec program in **Top 6 Tips for Explaining Why Your Application Security Journey Is Just Beginning.**

HOW TO GET EXECUTIVE SUPPORT

NYSE Governance Services, in partnership with Veracode, recently surveyed nearly 200 directors of public companies representing a variety of industries — including financial services, technology and health care — to discover how they view cybersecurity in the boardroom.

When asked to rank their biggest cybersecurity fears, 41 percent of directors said they're most worried about brand damage. Another 47 percent are nearly equally split between concern over theft of corporate intellectual property (such as strategic plans and proprietary designs) — leading to a loss of competitive advantage — and the total cost of responding to a breach (including cleanup, lawsuits, forensics and credit reporting costs).



When asked how they'd like cybersecurity information to be presented, nearly two-thirds of respondents indicated a strong preference for either risk metrics or high-level strategy descriptions.

It's clear that CISOs should be speaking to the board in terms that directors understand, such as by using risk benchmarks compared to industry peers and talking about breaches in similar industries — rather than by describing specific security technologies.

Get more details on this NYSE/Veracode survey report and its findings in our webinar, Understanding the Board's Perspective on Security.

Stats That Make the AppSec Case

85%

of applications that Veracode scanned in a recent 12-month period had at least one vulnerability on initial scan
State of Software Security v9

88%

of Java applications that Veracode scanned in a recent 12-month period had at least one flaw in a component
State of Software Security v9

$40%

Web application attacks remain the most frequent incident pattern in confirmed breaches.
2018 Verizon Data Breach Investigations Report

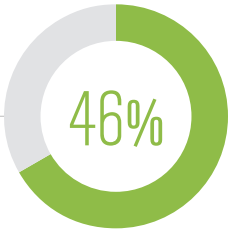
$6.0+

The global cost of cybercrime is predicted to cost the world more than $6 trillion annually by 2021
2017 Cybercrime Report, Cybersecurity Ventures

"Know your audience when speaking to the board about security. Do not use acronyms — think 'denial of service,' not DDoS. Use visuals instead of text, use analogies, and always use numbers, especially dollars if possible, such as losses from public data breaches. Bottom line: They want to know what are the odds our company will experience a damaging security breach and what are we doing to prevent that."

Chris Wysopal
Veracode
Co-Founder
and CTO

Another recent study that Veracode conducted reinforces the idea that you get the board's attention with stats and facts about the bottom line and brand damage. Our survey with YouGov questioned more than 1,000 business leaders across the UK, U.S. and Germany about their company's digital transformation initiatives and understanding of cybersecurity. Business leaders recommended the following approaches when talking to the board about cybersecurity initiatives:



Mention the money: Forty-six percent of business leaders in the U.S. stated that highlighting the cost of a breach, determined by a standard metric and cost of past breaches, will engage the board.

Point out the personal pain: More than a third of business leaders (38 percent) reported that giving senior executives examples of the personal brand damage that can come as a result of a data breach is an effective strategy for engaging them with cybersecurity. Highlighting the threat to executive jobs was also a commonly shared suggestion, with 35 percent of business leaders across all regions suggesting this would get board members sitting up and listening.

Need more specifics you can bring to the board? Get clear stats and facts to help you make a compelling case for AppSec spend in **How to Convince the Board That AppSec Is Your Most Productive Spend.**

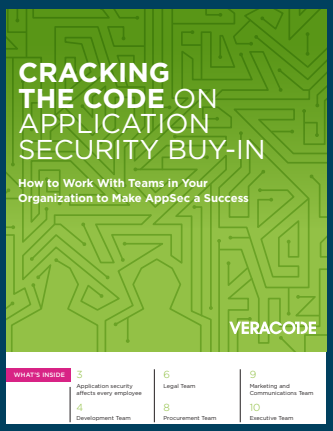
DEVELOPMENT TEAM

WHY YOU NEED DEVELOPER BUY-IN

To ensure the success of your application security initiative, it's essential to work closely with your developers so they understand the guidelines, strategies, policies, procedures and security risks involved with application security. What's more, they must be prepared and equipped to operate securely within their particular development processes.

Your application security program affects the development team more so than any other team in your organization. An advanced application security program requires security to be built into the software development lifecycle, and, as such, a poorly implemented application security program has the potential to disrupt the development team's day-to-day work.

Development teams' biggest fear when they hear their organization will enact an application security assessment program is that their development efforts will be slowed down. This team can be the biggest barrier to the success of the program because if they don't follow the protocol set forth by the program plan, the security team will be unable to demonstrate the value of the plan.



DOWNLOAD

Cracking the Code on Application Security Buy-In provides more tips and advice on getting AppSec support from various teams in your organization — including to-do lists and lists of questions to ask and be prepared to answer.

"From my own experience, I know I am less likely to balk at change if I am part of the conversation on how the change should occur. I think that is just human nature. Realizing this, it only made sense to work with the developers and product management rather than dictate how we would go about integrating application security into our development processes. In doing so, I was able to first understand how our development processes worked and how we came up with product requirements. With this understanding, I was able to work with the team to come up with realistic expectations around security."

Hailey Pobanz
Security Team,
DoubleDutch

Hear Hailey's whole story – How We Worked with Our Development Team to Make Security a Differentiator

HOW TO GET DEVELOPER SUPPORT

Bring them in early

Consult development teams early during the plan's conception and throughout its evolution. This way, the security team can ensure the assessment protocols don't disrupt the development lifecycle and, instead, enhance the development processes by making it easier for developers to find and remediate vulnerabilities.

When meeting with the development or development operations teams, be prepared with a set of best-practice guidelines you'd like to implement. However, don't present the guidelines as a set plan or strategy. Instead, describe your outline as a starting point for discussions, and ask for ideas on how this process can best fit into the existing development lifecycle. The less you have to change the current processes and the more you try to adapt your plan to fit their needs, the more likely its success.

Understand their priorities and processes

Make a concerted effort to learn as much as you can about your developers' priorities and processes. You have a much better chance of getting buy-in if you have a clear understanding of how the initiative will affect developers' routines.

This understanding will become more critical as DevOps emerges. As development processes change and evolve toward a DevSecOps model, the lines between development and security will blur. In fact, in a true DevSecOps world, developers would own security testing and the security team would take more of an enabling and supportive role.

Whatever development process your organization now follows, the future is DevSecOps, and the sooner security understands development — and development understands security — the more successful you'll be.

Find out more about increasing your knowledge of developer processes in our webinar, **How to Get the Best Out of DevSecOps: From Security's Perspective**.

Then find tools that work with those priorities and processes

Don't invest in an application security solution without developer input. And investigate AppSec tools that make it easy for developers to code securely. Look for solutions that are automated and integrate into the tools and processes developers are already using.

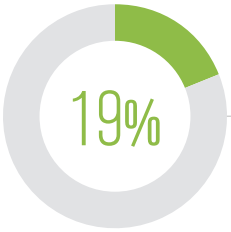
Get more details on developer-friendly AppSec tools in **Five Principles for Securing DevOps**.

Get them training

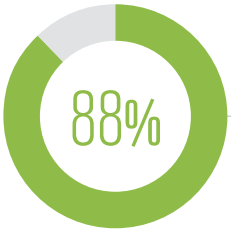
Most developers don't have security training. And without it, they'll struggle to get on board with your application security initiative.

A recent survey Veracode sponsored found that less than one in four developers or other IT pros were required to take a single college course on security. Meanwhile, once developers get on the job, employers aren't advancing their security training options, either. Approximately 68 percent of developers and IT pros say their organizations don't provide them with adequate training in application security.

The good news is that this is a problem with a solution. Our State of Software Security data shows that developer training leads to significant application security results.



Teams with developer eLearning in place improved developer fix rates by 19 percent.



Remediation coaching (consulting services that offer analysis and advice to developers alongside the scan results) improved fix rates by 88 percent.

VIDEO

Watch this video to hear what our Senior Vice President of Engineering has to say about developer security training.

MARKETING AND COMMUNICATIONS

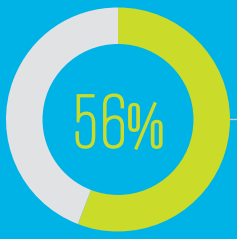
WHY YOU NEED MARKETING BUY-IN

Marketing departments are spinning up websites and landing pages, purchasing and creating mobile apps, hiring third-party contractors to help with automation, and purchasing applications from third-party vendors. In fact, marketing has now surpassed the IT department in technology spend. While these practices allow marketing departments to move quickly and reach their branding and demand-generation goals, they also introduce security risk. In an effort to move quickly, marketing departments often inadvertently operate around security procedures, and with applications being the No. 1 attack vector for cybercriminals, this can have dire consequences. Many of the breaches we hear about in the news are a result of a marketing-led program.

HOW TO GET MARKETING SUPPORT

The marketing and communications team doesn't set out to undermine your application security; they simply aren't aware of the dangers their actions create. When working with the marketing team, the most important thing you can do is to inform them of the risk and the policies you want to put in place. If you give them a set of guidelines to follow, they most likely will. As you create these guidelines, ask for feedback on how your teams can work together better.

Also consider enlisting the marketing department for help in communicating your AppSec program. By working with the marketing team to help you communicate your program plans, you will be better positioned for success.



56% of unsuccessful projects fail to meet their goals due to ineffective communication, according to Project Management Institute's *The Essential Role of Communications* report.

LEGAL TEAM

WHY YOU NEED LEGAL BUY-IN

Working with your legal team is especially important if you're including third-party applications in your security program. The legal team will need to be part of any contract negotiation to ensure your requests of vendors are legal, and your practices for testing third-party applications don't breach your customer contract. In addition, the legal team will help you craft language around your own security posture in situations where you're the software vendor.

HOW TO GET LEGAL SUPPORT

Perhaps better than any other constituent in your organization, the legal team understands the language of risk. As such, your conversations with this team should center on risk rather than technology and tactics used to assess the security of software. You should help this team understand best practices for these types of programs, and then iterate your program design based on their feedback.

Regulations from organizations, including FS-ISAC, the New York Department of Financial Services, NIST, PCI, MAS and more, now include **mandates surrounding the use of third-party applications** and/or open source code.

DOWNLOAD

Get all our best tips and advice on securing third-party applications and open source components in our Third-Party Software Security Toolkit.

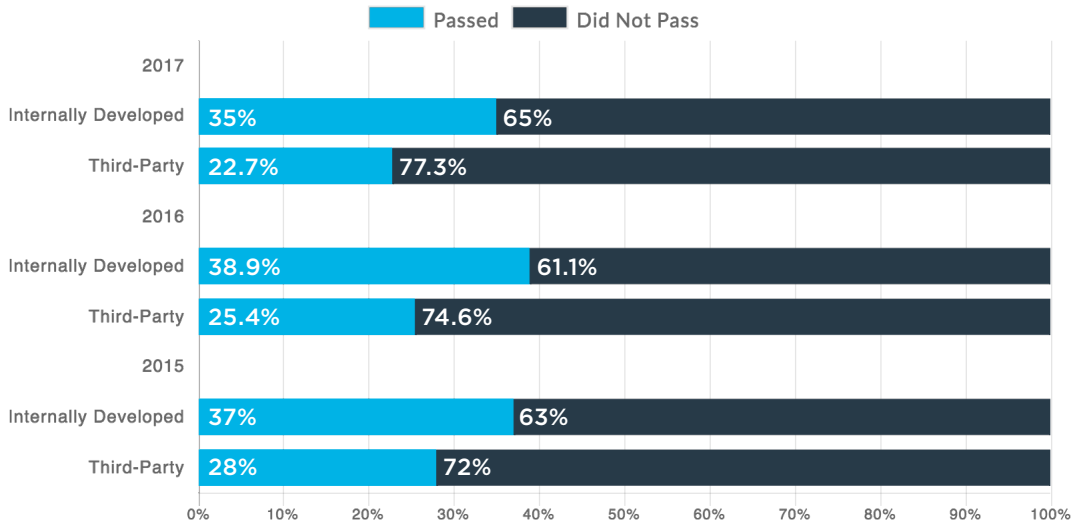
PROCUREMENT

WHY YOU NEED PROCUREMENT BUY-IN

The procurement team works with every department in your company, and they either report up to finance or legal. As with the legal team, application security programs impact this team the most when you implement a vendor application security policy, since they're the group that reviews vendor contracts. As a result, if you plan to include a vendor application security testing initiative as part of your overall application security program, you'll need to work with this team to modify contract templates and language.

Internally Developed vs. Third-Party (Commercial) Applications

Applications Passing OWASP Top 10 Policy



Source: *State of Software Security 2017*

HOW TO GET PROCUREMENT SUPPORT

The procurement team most likely reviews vendor contracts for various groups in your organization before they're signed. When reviewing contracts, they're looking for "red flags" that may pose a problem for your company in the future. These red flags include things like payment terms, product SLAs and so on. Work with this team by helping them identify the security posture language they should be looking for in any vendor contract. In addition, help the procurement team better understand their role in the application security process before you finalize your vendor application security testing.

Set yourself up for AppSec success by getting stakeholders on board early. Your program will stall before it starts without the full support of, at least, the executive and development teams. Especially with the rise of DevSecOps and the security "shift left," developers will increasingly play a key role in security — make sure they have the tools and skills they need to keep your program on track and your organization safe.

Contact us for help developing an application security plan and program.

ABOUT VERACODE

Veracode is a leader in helping organizations secure the software that powers their world. Veracode's SaaS platform and integrated solutions help security teams and software developers find and fix security-related defects at all points in the software development lifecycle, before they can be exploited by hackers. Our complete set of offerings help customers reduce the risk of data breaches, increase the speed of secure software delivery, meet compliance requirements, and cost effectively secure their software assets – whether that's software they make, buy or sell. Veracode serves over a thousand customers across a wide range of industries, including nearly one-third of the Fortune 100, three of the top four U.S. commercial banks and more than 20 of the Forbes 100 Most Valuable Brands. Learn more at veracode.com, on the Veracode Blog, and on Twitter.

VERACODE

RESOURCE ROUND-UP

TO GET EXECUTIVE BUY-IN:

- Find out how the board wants to be approached about cybersecurity: Cybersecurity in the Boardroom
- Get business leaders' tips on talking to the board about security: Securing the Digital Economy
- Gather up clear stats and facts to help you make a compelling case for AppSec spend: How to Convince the Board that AppSec Is Your Most Productive Spend

TO GET DEVELOPMENT BUY-IN:

- Watch this video to hear what our SVP of Engineering has to say about developer security training.
- Hear how one organization got their development team on board: How We Worked with Our Development Team to Make Security a Differentiator
- Get up to speed on developer processes and priorities: How to Get the Best Out of DevSecOps: From Security's Perspective.
- Get more details on developer-friendly AppSec: Five Principles for Securing DevOps.

TO GET ORGANIZATION-WIDE BUY-IN:

- Get practical tips and checklists on AppSec buy-in: Cracking the Code on Application Security Buy-In