JOINING FORCES

Why Your Application Security Initiative Needs Stakeholder Buy-In

GAINING BUY-IN FOR APPLICATION SECURITY FROM DIFFERENT GROUPS IN YOUR ORGANIZATION IS ESSENTIAL FOR **THE SUCCESS** OF YOUR PROGRAM.

VERACODE

INTRODUCTION

As organizations wade deeper into the digital age, it's clear that robust security is at the center of everything. Cyberattacks are on the rise, valuable data and intellectual property are increasingly at risk, and brand reputation and revenues are on the line. Yet, despite enterprise leaders directing money and resources to protecting networks and hardware, organizations are often left with significant gaps and vulnerabilities. One key area that's often overlooked: application security. **Recent studies indicate that attacks on the application layer are growing by more than 25 percent annually.**[1] Not only that, but the most recent numbers show that the estimated financial loss from 700 million compromised records is right around $400 million.[2]

MANY ENTERPRISE LEADERS MISTAKENLY BELIEVE THAT APPLICATION SECURITY IS TOO COMPLICATED, TIME-CONSUMING AND EXPENSIVE. WHAT'S MORE, GAINING SUPPORT AMONG DIVERSE GROUPS IN AN ORGANIZATION IS OFTEN DIFFICULT AND FRUSTRATING.

The ability to protect applications and software is nothing less than critical. Simply put: Application security is the final and most direct layer an organization relies on to shield its data. Unfortunately, it's also among the most underutilized methods of reducing risk. Many enterprise leaders mistakenly believe it's too complicated, time-consuming and expensive. What's more, gaining support among diverse groups in an organization is

often difficult and frustrating. But as information technology broadens and intersects with a growing array of functions and departments, the need for strong enterprise application security grows. A study conducted by the Project Management Institute (PMI) and Boston Consulting Group found that **79 percent of organizations with strong sponsorship and buy-in for ongoing initiatives are more likely to drive change in the organization.**[3]

TWEET THIS

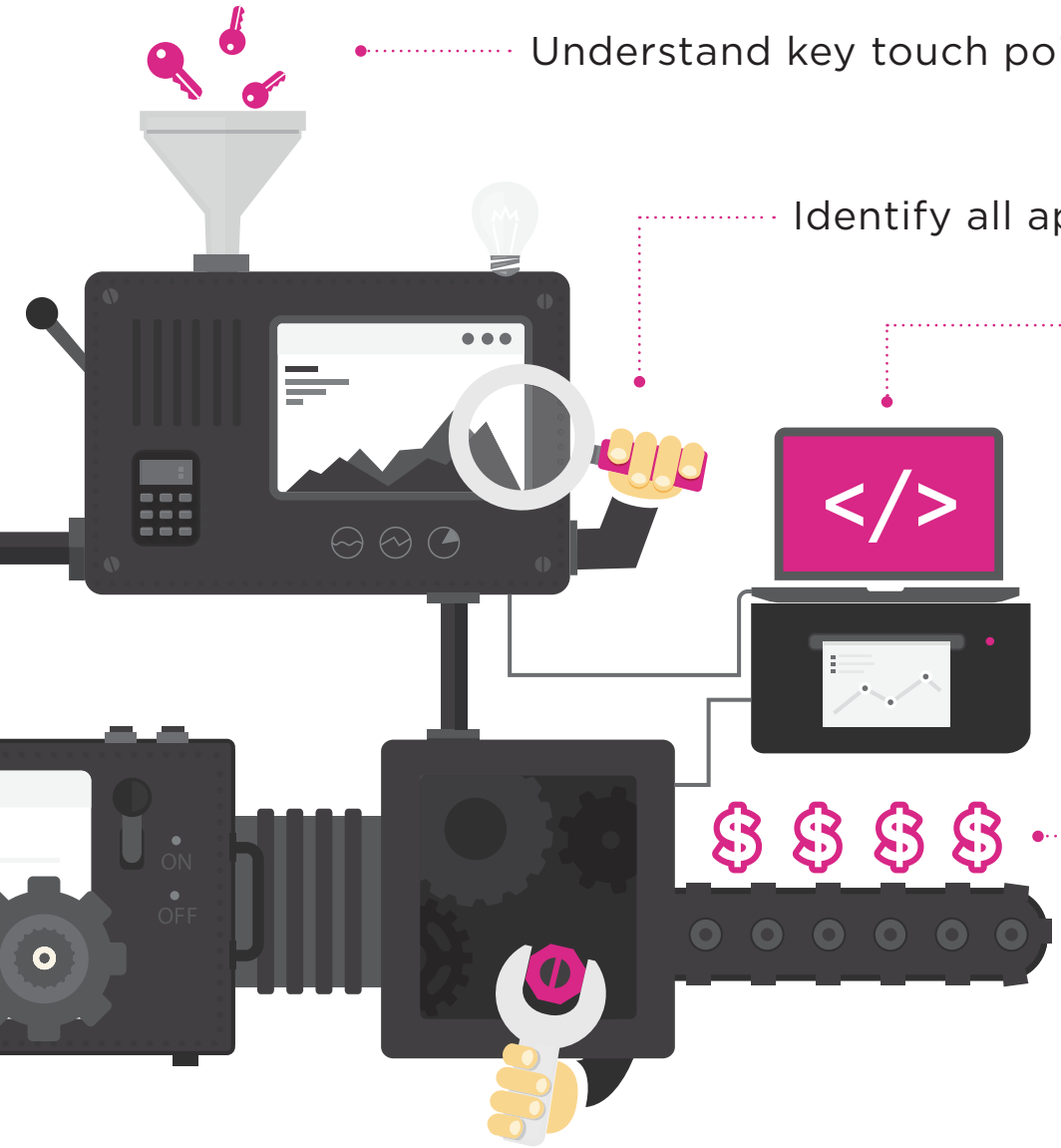
Mapping out an enterprise plan to build support for application security is paramount to the success of your program. It's important for key groups and departments in your organization — including the development team, legal department, contract management, marketing and communications, and the enterprise executive team — to play an active role in defining requirements, coordinating information and developing an overall framework that allows your organization to approach crucial processes and tasks as efficiently as possible. Among other things, this requires a strong governance model, the right technology, and communication and collaboration systems that allow your organization to operate at digital speed.

LEARN MORE

Are you getting resistance from the key departments in your organization about implementing an application security program? Team members may think it's too costly or will be difficult to manage, but that's just not the case. Find out what fallacies key departments may believe about application security — so you can help them understand the truth — in our handy guide, ***Application Security Fallacies and Realities***.

THE ROLES OF APPLICATION SECURITY

Gaps, breakdowns and glitches in cybersecurity aren't an accident — they're also largely avoidable. Although there's no way to eliminate all risk — today's security environment is incredibly complex and fast-changing — it's possible to mitigate your risk by addressing the task in a holistic and comprehensive way. Your enterprise must develop a structure that makes it possible to:



- Understand key touch points
- Identify all applications
- Recognize how to develop and code software in a way that's more secure, and also optimizes workflows and tasks that span departments and functions
- Allocate money and resources to your business's priorities
- Pinpoint where risks exist

A framework that fosters alignment among all key groups is imperative. As with any initiative, different stakeholders have different intrinsic needs and interests — and, in some cases, these ideas conflict with one another and with your organization's overall business and application security requirements.

EVEN THE BEST TOOLS AND SOLUTIONS ARE RENDERED INEFFECTIVE WITHOUT STRONG BUY-IN AND SUPPORT FROM THE KEY GROUPS WITHIN YOUR ENTERPRISE.

TWEET THIS

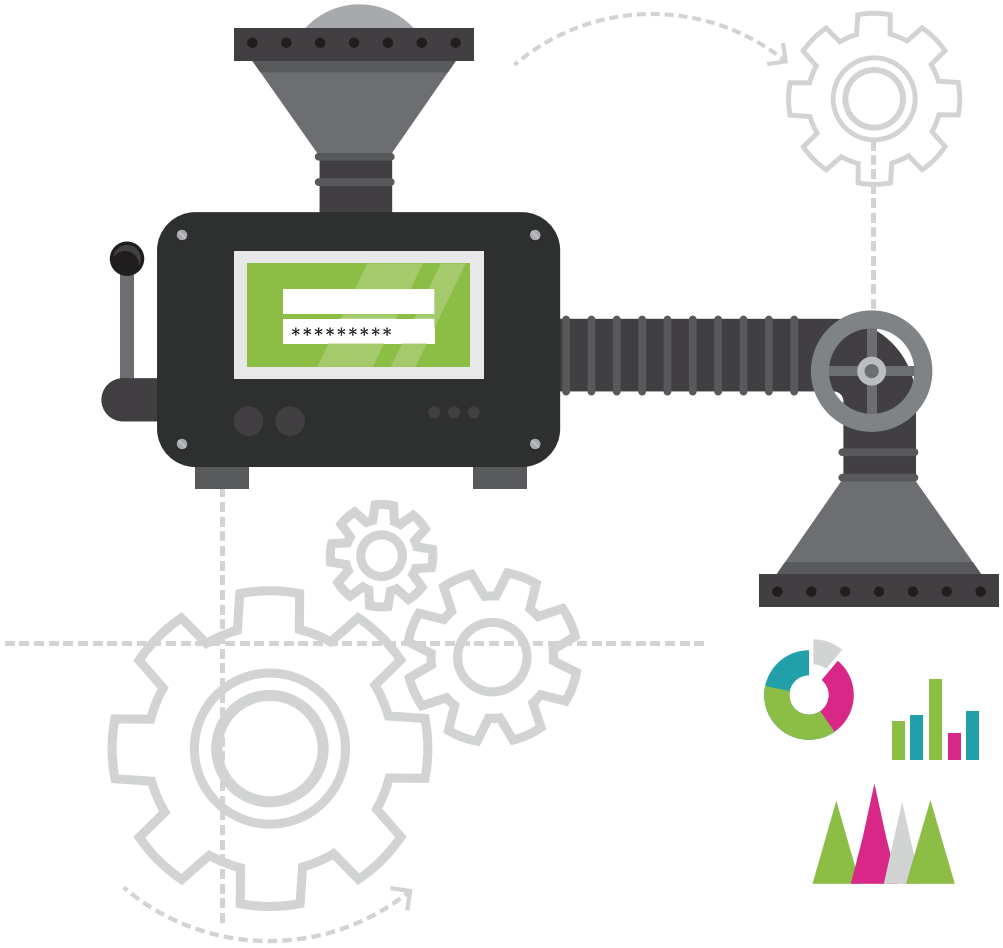
In addition, many general and technical areas require coordination. There's a need to establish clear and effective coding standards along with workflows that allow your entire enterprise — as well as its partners and customers — to stay in sync. As well, training and education help avoid conflicts and breakdowns that undermine an application security initiative.

For example, while everyone in your organization would most likely agree that strong security is essential and that application security is a key component, the practical reality is that an application security initiative may involve:

- Changes in interfaces
- New and different functionality
- Different legal requirements
- A change in contractual terms with vendors
- A different set of coding requirements for developers
- A need for your marketing and communications teams to develop new materials that help everyone in your company understand why the initiative is important and what they need to do to ensure success

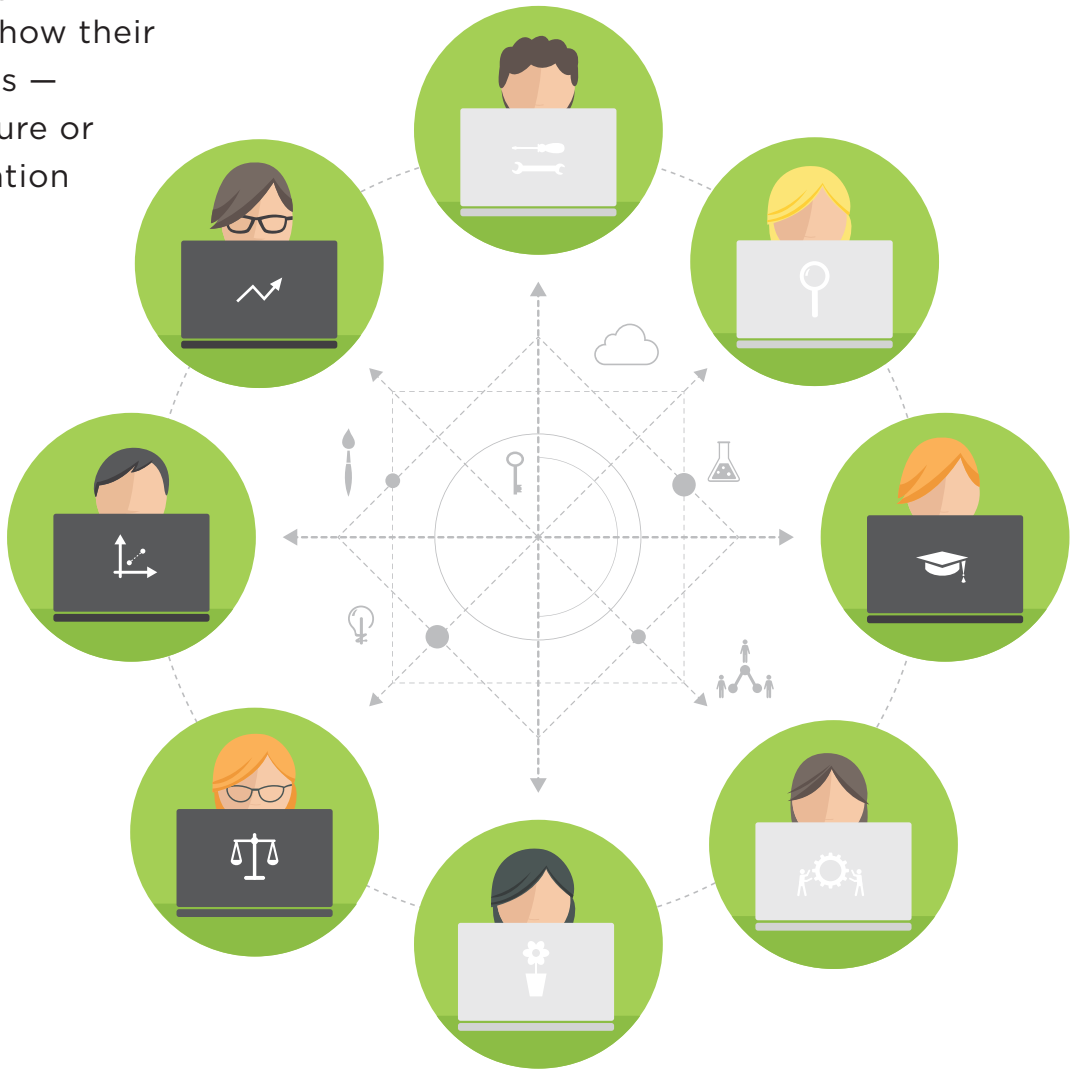
It's also important to recognize real-world issues, such as budget and resource constraints, that may extend to point-of-sales systems and enterprise devices.

The end goal is to build the mechanisms that support strong stakeholder alignment and consistent messaging. In the daily crush to get work completed and address the most pressing tasks, employees and others inside and outside your organization aren't necessarily focused on key criteria, goals and objectives that revolve around application security. Holding an occasional meeting to discuss the issue or issuing an infrequent memo won't get the job done. Application security is, ultimately, as much about people as it is about technical capabilities. Even the best tools and solutions are rendered ineffective without strong buy-in and support from the key groups within your enterprise.



PUTTING APPLICATION SECURITY TO WORK

A high level of alignment requires a clear understanding of the role that the different groups and departments in your organization play in achieving strong application security. Your organization must move beyond tactical issues and methods and build a strategic framework that puts your company's interests ahead of any individuals, function or department. Achieving this outcome requires a clear understanding of the role that key groups play and how their actions — or inactions — contribute to the failure or success of an application security initiative.



THE EXECUTIVE TEAM

It's no secret that 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, and ensuring internal and regulatory compliance. In fact, the PMI study noted above found that **76 percent of organizations report that the role of the executive sponsor has grown more important over the past five years.**[4] Without their commitment, any initiative is destined for disappointment or outright failure. Yet attaining best-practice results is no simple task. Success spins a tight orbit around several core issues, including these:

- Strategic alignment
- Sponsorship across the enterprise
- Essential financial and human resources
- A framework for collaboration and communication
- An ongoing commitment and focus on the initiative
- A framework that makes the initiative viable and durable over the long haul

IT'S IMPORTANT THAT YOU IDENTIFY — AND, IF POSSIBLE, QUANTIFY — THE KEY FACTORS OF YOUR APPLICATION SECURITY PROGRAM THAT WILL CONTRIBUTE TO THE SUCCESS OF YOUR BUSINESS.

Too often, IT teams emphasize the technical benefits of application security and other tools. Unfortunately, this type of argument is typically lost on executive teams who are more heavily focused on business risks and value. As a result, it's important that you identify — and, if possible, quantify — the key factors of your application security program that will contribute to the success of your business. This will help your executive team better understand key responsibilities and guidelines, as well as the standards needed to promote and deliver accountability. One key to elevating performance to a best-practice level is to help your executive team recognize that the objective isn't to create perfect alignment — something that will almost certainly never occur — but instead support consistent and recurring alignment throughout your organization.

With a culture of accountability and responsibility in place, it's much easier to deal with the constant and ongoing changes that exist in application security. With a framework that makes the CISO an executive sponsor and a liaison between the executive team and others, your organization's leadership can effectively oversee strategic planning teams, a task force and program teams that will address the tactical side of your initiative. Your enterprise can move beyond a compliance-centric approach and broaden its initiative to reflect realistic problems and solutions.

KEY TAKEAWAYS

- Too often, IT teams emphasize only the technical benefits of application security.
- Help your executive team recognize that the objective is to support consistent and recurring alignment throughout your organization.
- Make the CISO an executive sponsor and a liaison between the executive team and others.

CONTRACT MANAGEMENT SPECIALISTS

Vigilance over terms and contracts is an essential piece of your application security puzzle. Contract management specialists perform essential functions, including ensuring that agreements contain adequate security provisions and that a vendor or customer doesn't redline out critical provisions or terms. But in order for this process to be effective, your enterprise can't depend solely on templates and boilerplate provisions. And you can't approach the task in a haphazard way. It's important that you understand the specifics of a business arrangement, as well as how particular software applications impact security and the business as a whole.

In the past, the responsibility for contract management often fell under the exclusive domain of the IT department. However, as IT purchases have become more decentralized, organizations have come to recognize that they must broaden and deepen the scope of contract arrangements and purchase arrangements. In the end, a high level of communication and coordination across your enterprise is paramount. Knowledge-sharing is one key to ensuring that groups make good purchase and coding decisions — and thus achieve maximum buy-in. Moreover, as Agile initiatives such as DevOps move into the mainstream, it's important that you have clear application security guidelines and maximum buy-in. Key players across your organization must understand approval and procurement processes, best practices and what leads to the best possible results.

KEY TAKEAWAYS

- The consumerization of IT means that IT departments no longer control the purchase of software, increasing risk at your enterprise.
- Your enterprise can't depend solely on templates and boilerplate provisions to protect your software.

DEVELOPMENT TEAM

The heart of any application security initiative resides with a company's development teams. That's because development teams are responsible for coding applications, connecting software through clouds and APIs, validating security and making regular and ongoing adjustments to software. What's more, as DevOps and other Agile initiatives take shape, there's a need to move faster and more efficiently than ever.

Without strong buy-in from this group, the risks of a breakdown or breach grow. As software development has become more complex — and software lifecycles have become more intertwined with business processes — clear guidelines, strategies, policies and procedures are paramount. Quality coding practices are nothing less than essential. With these in place, instead of meeting resistance, you'll see an eagerness on the part of your development team to embrace new and better approaches.

KEY TAKEAWAYS

- The rise of DevOps and Agile development processes means companies need to work with development teams to integrate security into the software development lifecycle.
- Your developers need to understand their role in the application security process and why key tasks and procedures are essential.

THE LEGAL DEPARTMENT

Application security involves far more than technical and practical capabilities. A strong legal framework that ensures compliance takes place across all levels of your enterprise is also crucial to success. Contractual obligations are at the heart of an effective application security strategy. Your enterprise must identify specific, pertinent legal issues, understand their immediate and long-term impact, and tie them into various lines of business — without introducing onerous requirements that interfere with your business.

A legal framework must span all the various stakeholders, including contract management specialists, marketing and communications professionals, the executive team and others, and ensure that all of these groups are connected at the most fundamental level. No less crucial: ensuring that legal compliance exists among your various suppliers, vendors and other partners. Typically, the legal team must play an active role in framing the issues that surround your application security contracts. Once the overall structure and tools are in place, legal can move into the background.

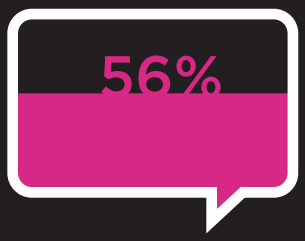
KEY TAKEAWAYS

- A strong legal framework that ensures compliance takes place across all levels of your enterprise is necessary for the success of your application security initiative.
- Working with your legal teams ensures legal compliance exists among your various suppliers, vendors and other partners.

MARKETING AND COMMUNICATIONS STAFF

An often-overlooked aspect of achieving buy-in is the role of your marketing and communications teams. These specialists play an active and ongoing role in ensuring that news and information flow from your executive suite to the rest of your organization — and even out to your business partners and customers. They also provide regular input and feedback to executives.

Without a strong communications framework and accurate information, anxiety, mistrust, misunderstandings and a variety of other problems typically emerge. In fact, the PMI study shows that 56 percent of unsuccessful projects fail to meet their goals due to ineffective communication. Consequently, it's essential for your marketing specialists to understand an initiative and its goals, as well as how to spread the word — and communicate both challenges and opportunities — in order to keep your entire organization up to date on key components and changes, and maximize engagement. What's more, in the event of a breach or other serious problem, it's critical to have a strategy and plan in place for dealing with the event.

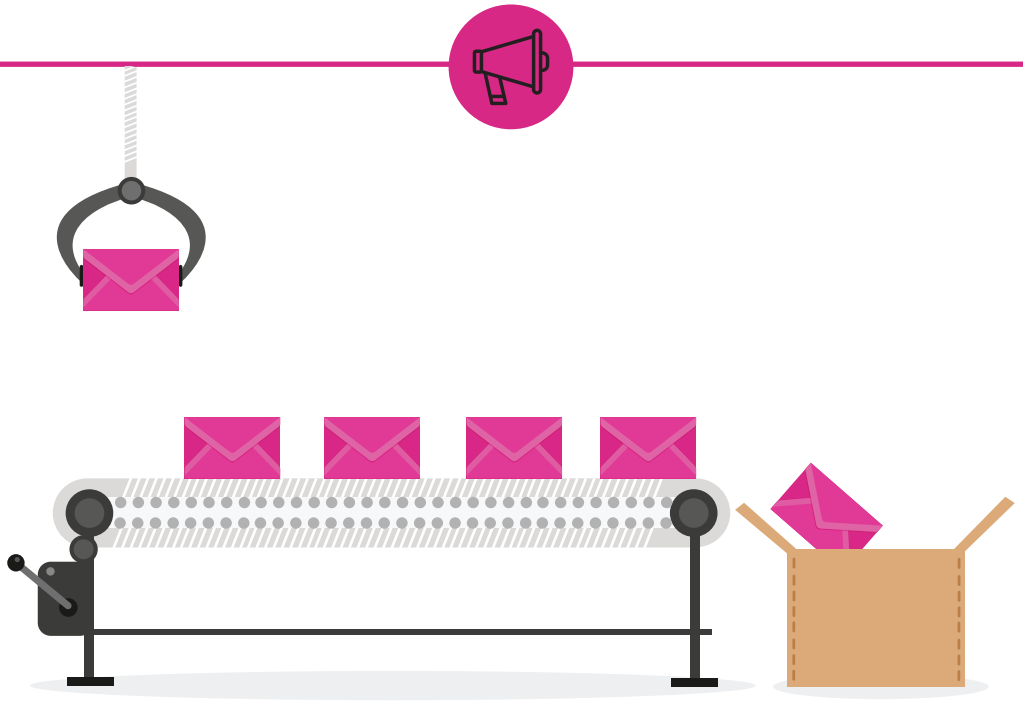


56 PERCENT OF UNSUCCESSFUL PROJECTS FAIL TO MEET THEIR GOALS DUE TO INEFFECTIVE COMMUNICATION.

Moreover, marketing efforts must span your company's different channels, such as its intranet, messaging systems and mobile devices, and tap a variety of methods, including e-mail, videos, podcasts, think papers, bulletins and even posts to social business and social media systems, in order to get the message across in a timely and efficient manner. Finally, marketing will help you gauge whether internal and external groups understand the messaging and are acting on it in a desirable way through the use of surveys, metrics and other tools. Having this marketing assistance is vital to the success of your initiative.

KEY TAKEAWAYS

- Involving your marketing and communications teams in the earliest stages of an application security program and throughout the software development lifecycle helps ensure its success.
- Make sure your marketing and communications teams are reaching out to both internal and external groups to help you communicate the key parts of your program.



10 KEY TAKEAWAYS

Here's what you need to know and do in order to achieve buy-in and attain best-practice results in application security:

1. Design and build a strategic framework that supports communication and collaboration across your enterprise and externally to your partners and others.
2. Have a task force and teams in place to oversee the initiative.
3. Create a governance model that allows your organization to control and manage myriad processes and tasks.
4. Attain a strong commitment from your executive team, including budgeting and resources needed to support the initiative enterprise-wide.
5. Put technology and tools in place to manage application security at a best-practice level.
6. Identify and implement quality coding practices for your development teams.
7. Develop a framework that allows your marketing and communications specialists to keep the organization informed and in sync.
8. Identify contractual and legal requirements and ensure that the entire organization is in lock-step when introducing new software or updating existing systems.
9. Build workflows and processes that streamline and simplify tasks.
10. Revisit the framework and the program's specific tools and systems on a regular basis.

CONCLUSION

The complexities of managing application security aren't lost on most executives. Many organizations and business leaders recognize that there's a need to take application security to a more advanced level and adopt a set of best practices that lead to greater alignment. However, translating the concept into a tangible, strategic and tactical framework is no simple task.

In order to develop an initiative that has company-wide backing, you need to make sure your application security program has:

- Strong executive support and oversight
- Clear standards for coding, contracts and legal matters
- The right technology and tools to manage the application security framework and data
- Streamlined and connected workflows
- A highly-coordinated internal marketing group that leads the enterprise down the road to greater alignment

And while getting buy-in from these stakeholders is essential, there are other teams in your organization, including finance, human resources and vendor relationship management, that you should consider working closely with so they're aware of and supporting your initiative.

In an era of growing risk, buy-in is essential to a complete application security framework.

[1] *Q3 2015 State of the Internet - Security Report*, Akamai, December 8, 2015.
[2] *2015 Data Breach Investigations Report*, Verizon, April 2015
[3] *Executive Sponsor Engagement: Top Driver of Project and Program Success.* Project Management Institute, October 2014.
[4] Ibid.
[5] Ibid.

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