TEAM EFFORT:
WHY STAKEHOLDER BUY-IN IS KEY TO APPLICATION SECURITY SUCCESS

No matter how much planning you've done or how many processes you've put in place, without stakeholder buy-in, your application security program is destined to fail. Here's what you need to know to make sure your efforts aren't in vain.

Recent studies indicate that attacks on the application layer are growing by more than 25 percent annually.[1] Equally alarming: Recent numbers show that the estimated financial loss from 700 million compromised records in a single year is in the vicinity of $400 million.[2]

But protecting assets and locking down valued data require more than security plans and software. There's a need to garner strong support and buy-in from the entire organization. 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 were more likely to drive change in the organization.[3]

A TEAM APPROACH IS ESSENTIAL

Application security touches various groups and departments in an enterprise. These include the executive team, the development team, contract management specialists, the legal department, and marketing and communications specialists. That's because application security typically involves:

- Changes in interfaces
- New and different functionality
- Different legal requirements
- Variations in contractual terms with vendors
- A different set of coding requirements for developers
- A need to develop materials that help all employees understand why the initiative is important and what they need to do to ensure its success
- An understanding of resource and budget constraints

When an enterprise is in sync and everyone is focused on a common set of goals, objectives, standards and criteria, the odds of locking down software and reducing vulnerabilities grow.

A FOCUS ON FUNCTIONS

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

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. They're integral to strategic alignment, sponsorship across the organization, delivering essential financial and human resources, and supporting a framework for collaboration and communication.

DEVELOPMENT TEAM

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 an Agile development framework, including DevOps.

CONTRACT MANAGEMENT SPECIALISTS

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. This group must fully understand the nuances and specifics of software and vendors in order to customize agreements. This reduces potential conflicts that can lead to coding and software vulnerabilities.

Find out how what challenges your peers are facing in getting AppSec buy-in. Check out the results of our recent survey, **Trends and Tactics: How IT Professionals Are Approaching AppSec Today.**

MARKETING AND COMMUNICATIONS STAFF

These specialists ensure that news and information about your application security initiative flow from the 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, and are able to gauge — using surveys, metrics and other tools —whether organizational buy-in is taking place. And because marketing departments are one of the largest consumers of applications, getting their buy-in, especially with third-party application security, is vital for your program's success.

THE LEGAL DEPARTMENT

A full understanding of legal issues and contractual obligations is crucial for application security success. This clear understanding leads to a governance model and policy management framework — as well as internal workflows and processes — that supports the security initiative. An effective legal framework must span all the various internal stakeholders and even cover suppliers, vendors and partners.

Organizations that build a framework for supporting application security — including a strong focus on stakeholder buy-in and keeping the organization in sync — are far more likely to emerge as best-practice leaders rather than laggards. Organizational buy-in is ultimately about reducing risk. It's nothing less than a matter of dollars and sense.

[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.

VERACODE