CRACKING THE CODE ON APPLICATION SECURITY BUY-IN

How to Work With Teams in Your Organization to Make AppSec a Success

WHAT'S INSIDE

INTRODUCTION

Securing the applications that run your business is now a critical task. Because applications help fuel innovation and boost productivity, organizations are using them in increasing numbers. However, the same applications that allow your business to run faster and smoother also introduce risk in the form of vulnerabilities. And this is why companies of all sizes need to develop application security (AppSec) programs.

Although every company building, buying or downloading applications should create an application security program, many are unsure where to start. Partnering with a trusted expert in AppSec can help reduce this complexity. Yet, even with a trusted partner, barriers will exist if you haven't worked with the correct teams to help build your strategy or properly socialize the strategy prior to its rollout.

- *Who are these teams?*
- *Why is their input so crucial to the success of the program?*
- *And, how do you work with each team to ensure you have the proper input and buy-in so that your program isn't derailed by interdepartmental dissent?*

This guide provides answers to these questions as well as practical advice for working across teams to ensure the success of your application security program.

APPLICATION SECURITY AFFECTS EVERY EMPLOYEE

Even the most well thought-out plan, with strong policies, guides and metrics, will fail if those policies are not 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 is unlike other forms of security in that it directly impacts the everyday 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 are slowing these employees down as well. Or worse, your policy may prohibit them from purchasing software that helps them do their job.

WHO IS MOST IMPACTED BY APPLICATION SECURITY?

Aside from the security team, which team carries the bulk of the burden when creating and implementing an application security program? What other teams are impacted? While the short answer is "everybody," you don't need to inform or consult with all teams early in the process. While we recommend informing your entire company once the plan is complete and in place, there are some departments you should consult during the development phase. These are development/DevOps, legal, procurement, marketing and communications and the executive teams. By including these departments in the planning phase, your strategy has a better chance of success, and you should have ready-made champions to help promote your strategy when it does go live.

INFORMATION SHEET
Why Application Security Programs Fail

✓ Why **you** need AppSec

Application security affects all employees, and, as a result, you need input and buy-in from different teams during the planning and rollout phases of your program.

DEVELOPMENT TEAM

WHITEPAPER
Putting Security into DevOps

WHITE PAPER
Secure Agile Development

Stake in the Game

Your application security program affects the development team more so than any other team in the 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 and DevOps 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 do not follow the protocol set forth by the program plan, the security team will be unable to demonstrate the value of the plan.

How to Work With the Development Team

Consult the development and DevOps teams early during the plan's conception and throughout its evolution. This way, the security team can ensure the assessment protocols do not disrupt the development lifecycle, and instead, enhance the development processes by making it easier for developers to find and remediate vulnerabilities. Learn more about how to integrate application security into an Agile development environment.

When meeting with the development or development operations teams, be prepared with a set of best-practice guidelines you'd like to implement. However, do not 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.

WEBINAR: Build Your Software Securely

By now, you are well aware of the implications of building and shipping insecure software. But it's challenging to keep pace with the rapidly changing development environment while ensuring security and compliance requirements are not compromised.

Questions to Ask

The development team can be a major ally in the creation of the program if you ask them the following questions:

1. Can you describe our software development lifecycle?
2. When do you currently assess the applications you are building for security?
3. How often are they tested?
4. Where do you think security assessments belong in the lifecycle?
5. How can we best fit into your existing process?
6. What are your biggest concerns about starting a program?
7. What would be the best way to test our strategy once we agree on the process?

While the responses to these questions may result in modifications of your plan, having this input is a crucial step in getting buy-in. By soliciting feedback and suggestions this early in the process, the development team will feel less like the application security program is an annoying edict they must follow, and more like it is a plan they had a hand in shaping. If you can accomplish this, the strategy is far more likely to succeed because the development team is more likely to follow proper procedures and support the plan.

Be prepared to answer the following questions:

1. How will the assessment process fit into the current development lifecycle (e.g., Agile, waterfall)?
2. How will this impact the development teams' productivity?
3. What training programs will be put in place to help the development team?

Benefits of Training

Consider security training to help the development team understand the different types of vulnerabilities and how to address them. eLearning can have a big impact on remediation. In fact, lack of developer knowledge of security is often cited as a barrier to producing more secure code. Our data shows that development organizations that leverage eLearning see a 30 percent improvement in fix rate compared to those that do not. It is important to note that this may be correlative rather than causative, since eLearning use is associated with other success strategies such as use of centralized policies, remediation coaching and other aspects of a systematic program. Read more in the *State of Software Security, Volume 6: Focus on Application Development.*

> **“Development organizations that leverage eLearning see a 30 percent improvement in fix rate compared to those that do not.”**
>
> ACCORDING TO VERACODE’S STATE OF SOFTWARE SECURITY, VOLUME 6: FOCUS ON APPLICATION DEVELOPMENT
>
> **TWEET THIS STAT**

LEGAL TEAM

Stake in the Game

Working with your legal team is especially important if you are 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 do not breach your customer contract. In addition, the legal team will help you craft language around your own security posture in situations where you are the software vendor.

How to Work With the Legal Team

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.

STATS TO GAIN BUY-IN

Organizations using remediation coaching services (“readout calls”) improve code security by a factor of 2.5x compared to those that choose to do it on their own.

STATE OF SOFTWARE SECURITY, VOLUME 6

61%

of development teams are not measured for compliance with secure architecture standards.

THE STATE OF APPLICATION SECURITY, PONEMON INSTITUTE, AUGUST 2013

REPORT
State of Software Security Report: Focus on Industry Verticals

STATS TO GAIN BUY-IN

84%

of organizations that suffered a data breach were out of compliance with application-layer security controls (PCI-DSS Requirement 6) — compared to an average of only 47% of all organizations assessed by Verizon QSAs in 2013. This suggests a strong correlation between the likelihood of suffering a data breach and non-compliance with application security.

VERIZON 2014 PCI COMPLIANCE REPORT

When working with the legal team to create vendor security contracts, start by:

☑ Making it clear what you are trying to accomplish in creating a vendor application security testing program.

☑ Providing examples of best practices and language used by other companies. You can get this information from your application security partner.

☑ Providing examples of what you would like your policy to look like, and how it would be enforced, and then ask for feedback on whether your standards are permitted by law.

For contracts or documents attesting to the security of the software your company is building, be prepared with:

☑ The standards you plan to adhere to (we recommend OWASP Top 10)

☑ A set of industry standards and benchmarks to demonstrate where your plan will fall in terms of industry standards

☑ Sample contract language you wish to use in your customer contracts

☑ SLA standards your plan will adhere to for patching if vulnerabilities are found

Questions to Ask

While you should come to any discussion with your legal team prepared with goals, examples of best practices and an outline of what you'd like your plan to look like, you should also come prepared with questions. This way, you can be sure your legal team has given you everything you need to ensure your contract language is correct.

1. Does using language that attests to the security of our products in customer contracts put us at risk in the event our software is deemed to be the root of a breach?
2. How can we mitigate that risk?
3. Given the language in our customer contracts, will our plan for assessing the security of our vendors' applications put us in breach of contract? How can we work with our vendors in the future to make sure that isn't the case?

Large organizations have a 75% chance of being breached via an application-layer attack.

VERIZON DATA BREACH INVESTIGATIONS REPORT (DBIR), DECEMBER 2012 PRESS RELEASE

PROCUREMENT TEAM

Stake in the Game

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 are 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, then you will need to work with this team to modify contract templates and language.

How to Work With the Procurement Team

The procurement team most likely reviews vendor contracts for various groups in the organization before they are signed. When reviewing contracts, they are 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 program by:

- ☑ Helping them understand why you are creating a vendor application security program.
- ☑ Describing the type of language they should be looking for in a contract by providing examples.
- ☑ Providing examples of language they may want to add to vendor contracts as part of the negotiation process.

Questions to Ask

1. What kinds of issues or language are you currently reviewing contracts for?
2. Are you able to reject contracts based on missing criteria?
3. How can we include security posture as part of our purchasing requirements?

STATS TO GAIN BUY-IN

60%

of organizations will suffer a security breach in 2015.

A FORRESTER PREDICTION

WHITEPAPER

Appropriate Software Security Control Types

A large and growing footprint of third-party software in the enterprise, regulatory bodies such as the OCC and industry organizations such as FS-ISAC, OWASP, NIST and the PCI Security Standards Council are now placing increased focus on controls to mitigate the risks introduced by third-party software.

MARKETING AND COMMUNICATIONS

Ask the marketing team to help you write company communications regarding new policies and guidelines and to help you draft presentations on your program's progress.

Stake in the Game

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 number-one 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 Work With the Marketing and Communications Team

The marketing and communications team does not 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 into 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.

Some of the items you'll want to discuss include:

1. The importance of assessing web applications for security prior to launch
2. The process the marketing department uses for evaluating vendors and for purchasing software
3. The policy you would like to enact for software purchases

However, in addition to needing marketing and communications' cooperation, they can also be a great ally. One area where security in general has faltered is in communicating the AppSec plan and its successes. By working with the marketing team to help you communicate your program plans and then successes, you will be better positioned for success.

STATS TO GAIN BUY-IN

56%

of unsuccessful projects fail to meet their goals due to ineffective communication.

ACCORDING TO PROJECT MANAGEMENT INSTITUTE'S ESSENTIAL ROLE OF COMMUNICATIONS REPORT

17.65%

increase in distributed denial of service (DDoS) attacks targeting the application layer in Q2 2015.

ACCORDING TO AKAMAI'S Q2 2015 "STATE OF THE INTERNET SECURITY REPORT" COMPARED TO Q1 2015

DID YOU KNOW?

In 2014 alone, there were eight major breaches through the application layer, resulting in more than 450 million personal or financial records stolen.

Questions to Ask

1. How will these policies impact your productivity?
2. How do you typically evaluate vendors and build web applications?
3. Are you able to help us communicate our plan to the rest of the organization?

Be prepared to answer:

1. Why are we assessing the security of the software we are buying?
2. From whom should I get approval for software purchases?
3. What is the process for purchasing software?
4. What about software we already purchased?

EXECUTIVE TEAM

Stake in the Game

The executive team's main concern around any new initiative is how it will impact the bottom line. It is the executive team's responsibility to ensure the company is operating efficiently as well as securely.

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.

How to Work With the Executive Team

When working with the C-suite around application security, the key is to focus on the benefits to the organization, rather than the technology or technical details of the program. For the C-suite, the main concern is the cost-benefit ratio. As such, provide information around how the assessment cycle will speed up development and reduce the cost of remediating vulnerabilities post-production. The conversation should also include information about the risk that vulnerabilities in the application layer pose to the organization, and how reducing this risk will ultimately save the company money and time. Always consider the information that a member of the C-suite would bring to the board.

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. Learn more about the board's perspective on application security.

Be prepared to answer the following questions:

1. What does our risk posture look like now?
2. Why should we invest in application security as opposed to other forms of cybersecurity?
3. What metrics will you use to demonstrate progress?

LEARN MORE: WEB ARTICLE

Benchmarking Your Industry in Today's Software Security Landscape

STATS TO GAIN BUY-IN

35%

of breaches are web application attacks, one of the most frequent patterns confirmed in breaches.

VERIZON DATA BREACH INVESTIGATION REPORT

CONCLUSION

Getting buy-in for your application security program is a key step many enterprises skip. However, creating a plan, even an advanced one, without working with key stakeholders is a recipe for a failed program. Application security touches more teams than the typical security program, and, as a result, if the teams impacted by your program feel they are being dictated to and didn't have their voices heard during the planning process, they are unlikely to comply with the regulations or guidelines you put in place. Similarly, if you do not communicate the program properly to the entire organization, you could find that most of your organization is inadvertently introducing the very risk you are attempting to avoid.

By working with the teams outlined above, you are taking a major step in ensuring the program that you so carefully crafted doesn't end up as a cut expense the following year. Instead, the positive results you achieve by working across your enterprise may result in an increased investment in application security, allowing your program to grow.

LOVE TO LEARN ABOUT APPLICATION SECURITY?

Get all the latest news, tips and articles delivered right to your inbox.

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.*

VERACODE

The Most Powerful Application
Security Platform on the Planet