SELLING YOUR ORGANIZATION ON APPLICATION SECURITY

Navigating a new era of cyberthreats

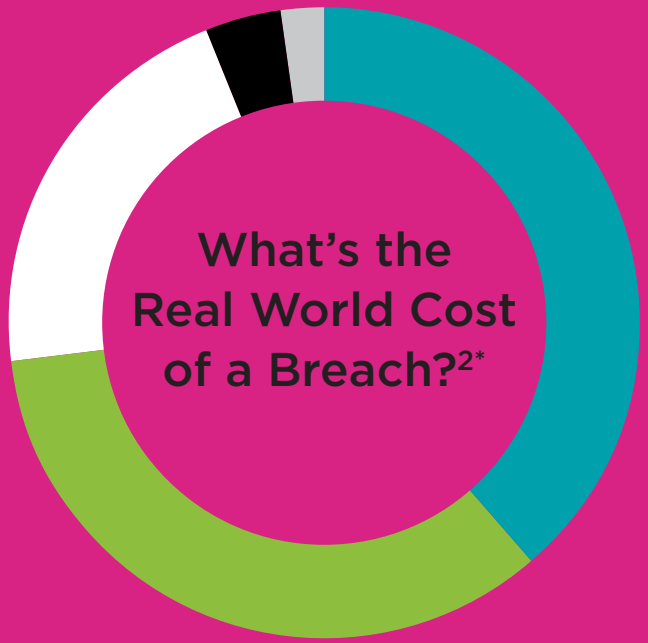
VERACODE

It's no secret that cyberattacks place organizations large and small at risk. Although these events are an inescapable piece of today's business puzzle, many breaches and breakdowns are avoidable.

An often-overlooked aspect is reducing risk in application security. By securing applications and creating a framework that supports consistent software and coding standards, an enterprise is better equipped to shield its data, information and intellectual property.

Cyber risk is no small problem: Losses from breaches exceed **US $400 million** annually.[1] But using a best-practices approach requires more than great tools and technologies. There's a need to achieve strong buy-in from five key groups and functions within the enterprise:

TWEET THIS



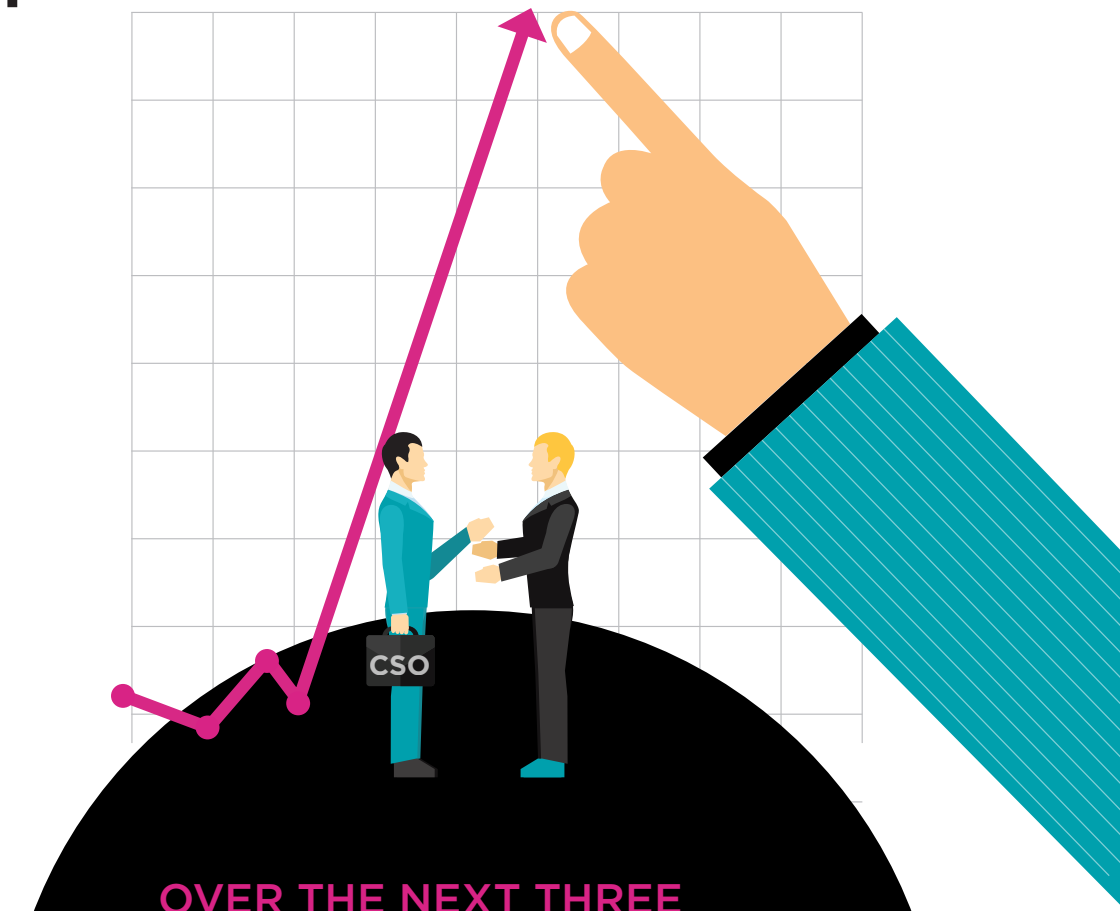
* Note that percentages add up to 101% due to study sponsor's use of rounding.

THE EXECUTIVE TEAM

Gaining support for your application security initiative among your board of directors, C-Suite and other key players means leaving the bits and bytes discussion behind and establishing a business case — along with quantifiable data — that focuses on value, cost and risk.

It's also imperative that your enterprise achieves strategic alignment across groups, sponsorship across the organization, essential budgeting support, the human resources necessary to achieve results, and an environment that promotes communication and collaboration.

This approach, which includes a CISO overseeing the task and serving as the liaison among groups, allows the organization to deploy effective program teams and create strong and consistent alignment.



OVER THE NEXT THREE YEARS, THE TIME CSOs WILL SPEND ADVISING BUSINESS EXECUTIVES IS ANTICIPATED TO INCREASE BY 79%.[3]

TWEET THIS

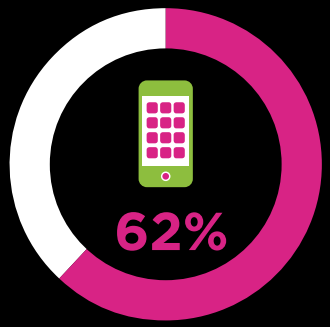
CONTRACT MANAGEMENT SPECIALISTS

Terms and agreements are the foundation of a strong application security framework and total organizational buy-in. As a result, it's vital to get your contract management specialists on board so there are overarching controls in place along with provisions that prevent groups from redlining critical terms and conditions.

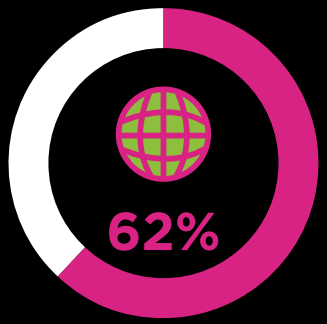
When contract managers effectively support application management and application security, the task becomes a strategic function that's tightly integrated across the enterprise. This leads to broader and deeper software controls and fewer gaps and vulnerabilities.

Security Risks Exist Across the Enterprise[4]

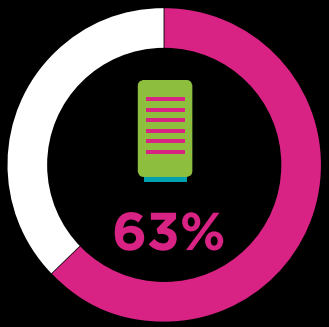
On average, almost two-thirds of all internally developed enterprise applications remain untested for security vulnerabilities. This category is composed of four key groups:



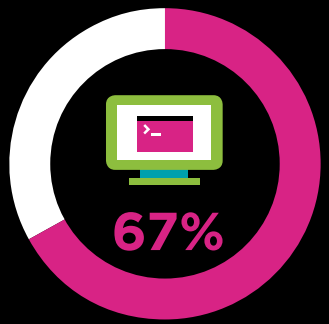
Mobile Applications not tested for security vulnerabilities



Web Applications not tested for security vulnerabilities



Client/Server Applications not tested for security vulnerabilities



Terminal Applications not tested for security vulnerabilities

DEVELOPMENT TEAMS

The success of today's digital enterprise revolves heavily around software and coding. As a result, achieving buy-in among development teams is critical. These groups must tie together diverse groups of applications, APIs and other open-source libraries, public and private clouds, and more. Without consistent standards and a strong commitment to application security, the task is next to impossible.

The upshot? Development teams must have quick and easy access to guidelines, policies and procedures. The result is more consistent coding and far more integrated software lifecycles that ultimately lead to better application security.

A TYPICAL U.S. $500 MILLION-PLUS ENTERPRISE RELIES ON MORE THAN 3,079 APPLICATIONS THAT IT HAS DEVELOPED INTERNALLY.[5]

TWEET THIS

95% OF BREACHES INVOLVE HARVESTING CREDENTIALS STOLEN FROM CUSTOMER DEVICES AND THEN LOGGING INTO WEB APPLICATIONS WITH THEM.[6]

THE LEGAL DEPARTMENT

Over the past decade, software procurement and development have become incredibly complex tasks. It's essential to build in mechanisms that boost compliance internally, within an industry and for government mandates and regulations.

A legal department is at the center of all this, making their buy-in essential to your application security program. The legal team will help your enterprise — and your vendors — establish workable conditions and ensure that all parties abide by contractual obligations. They must also protect the organization from unnecessary legal exposure.

INTERNALLY DEVELOPED APPLICATION PORTFOLIOS ARE GROWING AT A RAPID 12% ANNUAL RATE. THIS TRANSLATES INTO AN AVERAGE OF 371 NEW APPLICATIONS FOR A TYPICAL ENTERPRISE WITHIN THE NEXT YEAR.[7]

TWEET THIS

MARKETING AND COMMUNICATIONS SPECIALISTS

Capturing the hearts and minds of key players doesn't happen on its own. Even the best tools, most efficient processes and strongest executive support aren't enough to guarantee success.

Consider this: A Project Management Institute (PMI) study found that **56 percent of unsuccessful projects fail to meet their goals due to ineffective communication.**[8] This points directly to the need for support from internal marketing and communications teams, who will help oversee your initiative and keep news and information flowing both upstream to senior executives and downstream to the enterprise. They must also tap surveys and metrics to understand whether the message is getting across and buy-in is taking place.

TWEET THIS

AN ENTERPRISE MUST DEVELOP A STRATEGIC PLAN ALONG WITH THE TECHNOLOGY, PROCESSES AND COMMUNICATION NEEDED TO FULLY SUPPORT AN APPLICATION SECURITY INITIATIVE.

PUTTING IT ALL TO WORK

Having your key stakeholders recognize that application security is a business imperative is a key step in building a cybersecurity framework for the present and the future.

Your enterprise must develop a strategic plan along with the technology and processes to fully support application security. Your leaders must connect and integrate key groups while establishing robust communication channels that keep everyone informed and engaged.

With this foundation in place, it's possible to achieve total buy-in and tackle application security in a holistic and highly effective way. The result is a business that's fully equipped to deal with today's opportunities and challenges.

24% OF ORGANIZATIONS SUFFERING A BREACH REPORT FINANCIAL LOSSES OF $100,000 OR MORE, AND 7% REPORT LOSSES OF MORE THAN $10 MILLION.[9]

MORE THAN HALF OF ALL RESPONDENTS IN A RECENT SURVEY EXPECT SPENDING ON APPLICATION SECURITY TO INCREASE OVER THE NEXT YEAR. WITH SO MUCH ON THE LINE, GETTING STAKEHOLDER BUY-IN IS NOTHING LESS THAN CRITICAL TO THE SUCCESS OF YOUR INITIATIVE.[10]

To learn more about making the case for application security, check out our new guide, **"Top 6 Tips for Explaining Why Your Application Security Journey Is Just Beginning."**

DOWNLOAD

LOVE TO LEARN MORE ABOUT APPLICATION SECURITY?

Get all the latest news, tips and articles delivered right to your inbox by subscribing to our blog.

Subscribe Now

ABOUT VERACODE

Veracode is a leader in securing web, mobile and third-party applications for the world's largest global enterprises. By enabling organizations to rapidly identify and remediate application-layer threats before cyberattackers can exploit them, Veracode helps enterprises speed their innovations to market — without compromising security.

Veracode's powerful cloud-based platform, deep security expertise and systematic, policy-based approach provide enterprises with a simpler and more scalable way to reduce application-layer risk across their global software infrastructures.

Veracode serves hundreds of 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 Forbes' 100 Most Valuable Brands. Learn more at **www.veracode.com**, on the Veracode **blog** and on **Twitter**.

1 *2015 Data Breach Investigations Report*, Verizon, April 2015.
2 *2015 Cost of Cyber Crime Study: Global*, Ponemon Institute, October 2015.
3 "State of the CSO 2014," CSO Magazine, 2014.
4 *The Application Enterprise Landscape,* IDG Research, May-Aug 2014.
5 Ibid.
6 Ibid.
7 Ibid.
8 *Executive Sponsor Engagement: Top Driver of Project and Program Success,* Project Management Institute, October, 2014.
9 *2014 Global State of Information Security Survey,* PriceWaterhouse Coopers, CIO Magazine & CSO Magazine, September 2013.
10 *2015 State of Application Security: Closing the Gap*, Sans Institute, May 2015.