Analyst Insight

Aberdeen Group
A Harte-Hanks Company

August 2011

Securing Your Applications: Get Started Now

If your organization hasn't gotten started yet in the area of application security – in spite of the **dynamic nature of the application security threat landscape**, the **size and diversity of your application software portfolio**, and the **significant financial impact of the average application security-related incident** – do it because of the **positive impact on your bottom line**. This Analyst Insight reviews several practical steps you can take to get started now.

Business Context: The Biggest No-Brainer in Security?

New headlines provide ongoing evidence that IT Security teams are losing the battle against attackers, reinforcing the need to address the security of enterprise applications. In the recent CitiGroup breach, for example, more than 200,000 cardholders had their names, email addresses, account numbers and transaction histories exposed as a result of a well-known application security vulnerability. As reported by the *New York Times*:

- *The data thieves were able to penetrate the bank's defenses by first logging on to the site reserved for its credit card customers. Once inside, they leapfrogged between the accounts of different Citi customers by inserting various account numbers into a string of text located in the browser's address bar. The hackers' code systems automatically repeated this exercise tens of thousands of times – allowing them to capture the confidential private data.*

In the language of the application security community, this is referred to as a *direct object reference*, which occurs when attackers are able to manipulate direct references to an internal implementation object (e.g., a file, directory or database key) to access unauthorized data. It's actually on the Top 10 list of web application security threats identified by the Open Web Application Security Project (OWASP).

But this Analyst Insight is not about fear-mongering or sensationalizing the latest headlines to gain your focus on securing your applications. It is about your organization's bottom line.

Why You Should Get Started Now

Aberdeen's benchmark study and several follow-on publications (see the *Related Research* section at the end of this report) showed that *all* respondents experienced a positive return on their annual investments in application security – not only the leading performers ("Best-in-Class"), but also the lagging performers ("Laggards").

Analyst Insight

Aberdeen's Analyst Insights provide the analyst perspective of the research as drawn from an aggregated view of surveys, interviews and analysis.

Top 10 Web Application Security Vulnerabilities

- √ Injections
- √ Cross-site scripting
- √ Authentication and session management
- √ Direct object references
- √ Cross-site request forgery
- √ Security misconfiguration
- √ Insecure cryptographic storage
- √ Failure to restrict URL access
- √ Insufficient transport layer protection
- √ Unvalidated redirects and forwards

Source: Open Web Application Security Project, 2010

How can this be?

- **The dynamic nature of the application security threat landscape** – industry sources note that nearly half of all reported security vulnerabilities are related to web applications, and companies are struggling to keep up not only with the well-known (such as the OWASP Top 10) but also with the newly emerging (such as vulnerabilities in applications for mobile platforms).
- **The size and diversity of the typical application software portfolio** – the average respondent in Aberdeen's study has deployed over 130 applications, the provenance of which ranges from internal development to outsourced development, systems integrator development, open source, Web 2.0, and commercial off the shelf.
- **The material impact of an actual security-related incident** – for all participants in this study, the average total cost of an actual application security incident was estimated at $300,000. This number takes on even greater significance when compared to the average total annual investment – including the people, the processes and the technologies – which was about $400,000.

Application security-related incidents have a *high probability* of occurrence, a *high frequency* of occurrence, and a *high financial impact* per occurrence. The average financial impact of a single occurrence is nearly as high as the total annual cost of initiatives to protect against them – and no matter which approach to protecting against them is taken, the average respondent successfully prevents multiple occurrences per year.

Determining the Best-in-Class

To distinguish Best-in-Class companies (top 20%) from Industry Average (middle 50%) and Laggard organizations (bottom 30%) in application security, Aberdeen used the year-over-year changes in the following:

√ Number of application security-related vulnerabilities

√ Number of audit deficiencies related to application security

√ Average time to remediate one critical application vulnerability

Over the last 12 months the top performers also experienced fewer actual data loss or data exposure incidents, as well as fewer audit deficiencies, related to application security.

Table 1: Top Performers Balance Both Efficiency and Effectiveness to Maximize Annual Returns

Assessing the Business Value Derived from Application Security	Best-in-Class	Industry Average	Laggards
Application vulnerabilities identified and remediated prior to deployment	88.3%	81.7%	76.6%
Application security-related incidents experienced in the last 12 months	3.9	6.3	11.1
Total annual cost of application security initiatives (includes all related costs for people, process, and technologies)	$350K	$330K	$480K
Annual cost of application security-related incidents *not avoided* (Note 1)	$1,180K	$1,900K	$3,330K
Annual cost of application security-related incidents *avoided* (Note 2)	$8,880K	$8,440K	$10,940K
Return on annual investment from application security initiatives	5.8	3.8	2.9

Note 1: the average total cost of an actual application security incident for participants in this study was estimated at $300,000
Note 2: assumes that the ratio of "avoided" to "not avoided" is in the same proportion as the application security vulnerabilities that were not identified and remediated prior to deployment
Source: Aberdeen Group, August 2010

Table 1 summarizes the evidence for Aberdeen's assertion that all respondents, from leading performers to lagging performers, realized a positive return on their annual investments in application security. Focusing on a comparison of leaders to laggards, we can see that the top performers:

- Identified and remediated a higher percentage of application vulnerabilities prior to their deployment
- Experienced fewer actual application security-related incidents in the last 12 months
- Spent less on the total annual cost of their application security initiatives (including all related costs for people, process, and technologies)

When you work out the math for an assessment of return on investment (see the sidebar for Aberdeen's simple approach), the clear takeaway from the numbers is that application security initiatives of all kinds represent extremely good business value. And as it turns out, taking steps towards implementing best practices in application security provides the potential for even stronger benefits and results. But as Lao-tzu has reminded us for more than 2,500 years now, "a journey of a thousand miles begins with a single step." In other words, **get started**.

So You've Decided to Get Started – Now What?

Based on the experiences and capabilities of the top performers, Aberdeen's research has identified several general steps to success. Let's examine each of them in turn.

Identify Your Application Portfolio

As mentioned above, the average respondent in Aberdeen's study currently supports a portfolio of over 130 deployed applications, which is growing year over year. The overall end-user population (including employees, contractors, business partners and customers) for these applications is also growing year-over-year, combining to increase significantly the number of potential attack vectors for Internet-facing enterprise applications. So the first – and hopefully obvious – step is to take stock of the inventory of applications you already have.

Identify Your Greatest Risks

Few companies have the resources to remediate all application security vulnerabilities at one time. And frankly, not all application security vulnerabilities are created equal (think back to the discussion about *probability* of occurrence, *frequency* of occurrence, and *financial impact* per occurrence). So the logical thing to do is to give the highest priority to the specific applications, or classes of applications, which represent the greatest risk. In fact, the leading performers are 2-times more likely than the laggards to take a risk-based approach.

Respondents in Aberdeen's study ranked *legacy applications with web-based front-ends*, *.NET-based* and *Java-based* web applications, and *Web 2.0* applications as the highest in their current assessment of application security risk. Given the increase of mobile devices (e.g., smartphones, tablets) in the

Assessing the Business Value

For the purposes of evaluating the business value of enterprise investments in application security initiatives, Aberdeen uses the following simple equation:

√ Total annual cost of application security-related incidents that were successfully avoided

divided by

√ Total annual cost of application security initiatives, **plus** the total annual cost of incidents that were *not* avoided

The denominator includes the total annual cost for the organization's application security initiatives; also in the denominator, however, are the total costs from incidents that were not avoided in the last 12 months, *in spite of* the investments in application security that have been made.

In the numerator are the best estimates for the total costs of incidents that *were* avoided in the last 12 months as a result of the organization's investments in application security – these may be difficult to come by, however, and imprecise at best.

For this reason, the most general way to think about this simple framework is that any investments in technologies and services that lower the total annual cost of the initiative (*efficiency*) and cause a greater shift from the denominator to the numerator in terms of incidents avoided (*effectiveness*) will have a strongly positive impact on the overall return on annual investment.

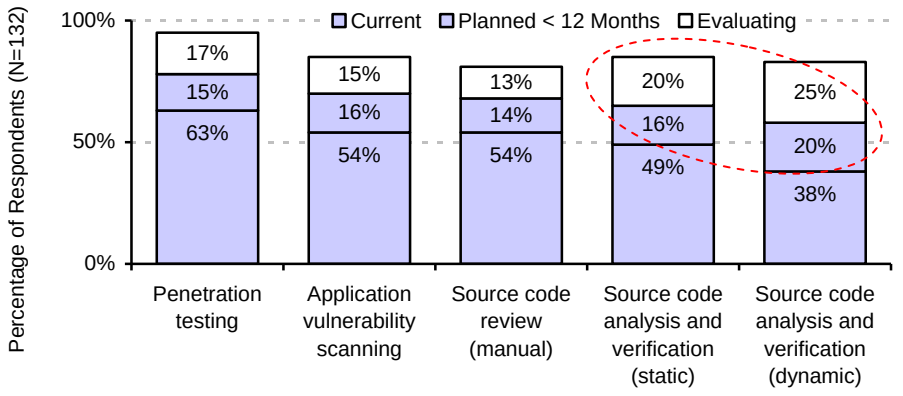
enterprise, Aberdeen also looks for *enterprise mobile applications* to jump to the top of this list in the near future.

"Crawl, Walk, Run" is almost always a smart approach to any enterprise-wide initiative – meaning start small, perhaps with a proof-of-concept for a specific application. Establish a track record of proven success, and then expand over time to protect your broader application portfolio.

Understand and Use the Tools at Your Disposal

For the majority of all respondents in Aberdeen's study, *penetration testing*, *application vulnerability scanning*, and *manual source code reviews* represent the most common techniques or technologies currently used in application security (Figure 1). Between 40% to 50% of companies are currently using *static source code analysis* or *dynamic source code analysis* – but when you look at the proportion of current evaluations, along with planned use in the next 12 months, the research indicates very strong, above-average market interest and near-term growth in these areas.

Figure 1: Tools in Your Toolbox: Current Use, Planned, Evaluating



Source: Aberdeen Group, December 2010

Knowing which technologies and tools are currently being used, planned for, and evaluated by all respondents is interesting, but what would be even more valuable is to have insight into which tools are associated with the companies that are *achieving better results* relative to their peers. One of the unique aspects of Aberdeen's benchmarking style of research is that it correlates performance (results) with current capabilities in people, process and technologies to provide these types of insights.

It turns out that the leading performers (Best-in-Class) are in fact strongly differentiated from the lagging performers (Laggards) in their current use of these tools, in combination with a corresponding commitment to secure application development practices. Aberdeen's research shows that *application vulnerability scanning*, *penetration testing*, *static source code analysis and verification*, and *dynamic source code analysis and verification* are the

technologies that most strongly differentiate the companies that achieved the best results.

Choose the Best Deployment Option

When you investigate specific solutions in this area, keep in mind that there are **multiple deployment options** – e.g., *on-premise software*, *on-demand solutions* (e.g., pay-as-you-go) or *software-as-a-service* (e.g., subscription-based, typically for a period of time). Part of your selection criteria may hinge on the availability of skilled security staff within your company; for example, on-demand testing-as-a-service may be the most cost-effective way to get started if you don't, while on-premise dynamic testing might be most appropriate if you do. Solution providers that offer you maximum flexibility of deployment options, along with outside expertise as you need it, are probably the smartest choices to ensure your success.

Establish Clear Ownership

If may sound obvious, but having an executive or team with clear ownership and accountability for an important enterprise-wide initiative such as application security is consistently correlated with the achievement of top results. This is sometimes referred to as the "one throat to choke" principle – and from experience, most of us can probably appreciate that when everybody is in charge, nobody is in charge. For example, is developer time better spent addressing high-risk vulnerabilities identified by proactive application vulnerability scanning and penetration testing – or adding features and accelerating release dates? Having clear ownership and accountability for application security can help to arrive at an acceptable balance between business context, risk-based business judgment, and overall management philosophy on what to address and when.

Identify the Vulnerabilities, and Prioritize the Remediation

We've already established that few organizations can invest the resources to fix all vulnerabilities with equal priority, so an efficient system of triage is essential. Logically the greatest risks, evaluated as a function of potential impact and likelihood of occurrence, should be remediated first. The application scanning and testing tools will help you identify what specific application vulnerabilities you have, and the tools in combination with your own experience and judgment will help you prioritize which vulnerabilities to address.

Partner Between IT Security and Application Development

Often, the IT Security team will be the ones to get started with application security, by applying scanning and testing technologies to the organization's portfolio of deployed applications. What you probably want to avoid is a scenario in which the IT Security team finds vulnerabilities and then "throws them over the wall" to be addressed by the Application Development team. As already noted, the developers already may be under direction to add features and accelerate release dates, as opposed to addressing

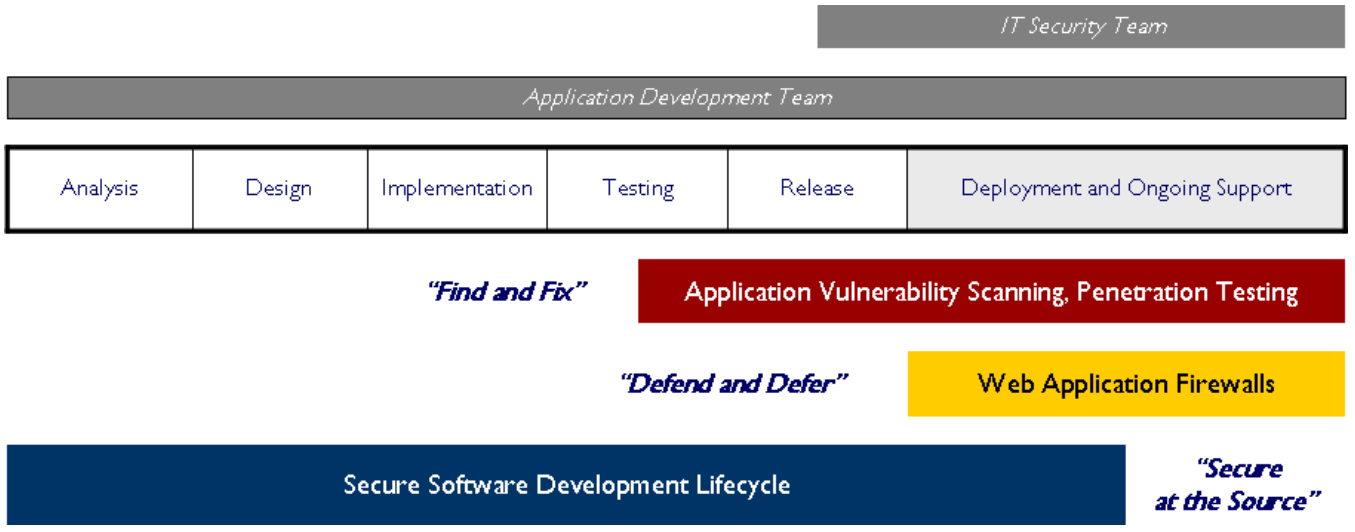
vulnerabilities that were identified by proactive scanning and testing. The best evidence that a partnership is in place is when IT Security and Application Development think not in terms of "us" and "them", but in terms of "we".

Well-defined communication channels between IT Security, operations and application development teams will improve both the efficiency and the effectiveness of identifying and remediating application security vulnerabilities. Two-thirds of the leading performers indicate this as a current capability, compared to less than half of the laggards.

Adopt a Primary Strategy

In the early phase of your initiative, you can use the results from proactive scanning and testing to provide concrete evidence to the Application Development team of the need for securing your applications. Eventually, however, you will have to get to the heart of the discussion, which is the question of *where* in the canonical software development lifecycle (SDLC) – *analysis*, *design*, *implementation*, *testing*, *release*, *deployment* and *ongoing support* – you feel that application security vulnerabilities are most appropriately identified and remediated (Figure 2).

Figure 2: Securing Your Applications, in Different Areas of the Software Development Lifecycle



Source: Aberdeen Group, September 2010

Aberdeen's research on this question is extremely clear: companies adopting the *Secure at the Source* strategy – i.e., the **integration of secure application development tools and practices into the software development lifecycle** – realized a greater return on their annual investment than either the *Find and Fix* or *Defend and Defer* approaches. Although the *Secure at the Source* approach is currently the least common to be implemented, Aberdeen's research confirms that it is maturing and transitioning from early adoption to mainstream use. Obviously this will not

happen overnight, but the research demonstrates that you should definitely begin your application security initiative with this end in mind.

Train the Developers

Unfortunately, education and training in application security policies and best practices is an area where there is virtually no distinction between the leaders and the laggards, which represents an immediate opportunity for improvement. The simple takeaway: don't just keep telling the developers that they're doing something wrong; make them aware of how to do it right!

Measure and Monitor to Communicate with Management

Management must not only establish application security as a priority, but also allocate the tools and resources necessary to pursue it successfully – the last thing any project needs is to be an "unfunded mandate." By providing the management team with visibility into actual application security incidents and the time and cost to remediate them, your business leaders will have the information and insights they need to ensure that resource allocation is consistent with the stated strategy. Three out of 5 leading performers do this, compared to just 2 out of 5 laggards.

Solutions Landscape (illustrative)

Solution providers associated with the *Secure at the Source* approach to application security range from service organizations to specialists to integrated application security suites from multi-billion dollar corporations; Table 2 provides an illustrative list.

Table 2: Solutions Landscape for Security and the Software Development Lifecycle (illustrative)

Company	Web Site	Solution(s)
Armorize	www.armorize.com	CodeSecure, SmartWAF, HackAlert
Aspect Security	www.aspectsecurity.com	Implementation, Verification and Management services
Coverity	www.coverity.com	Static Analysis, Dynamic Analysis, Build Analysis, Architecture Analysis
Electric Cloud	www.electric-cloud.com	ElectricCommander, ElectricAccelerator, ElectricInsight
HP Fortify	www.fortify.com www.hp.com	HP Fortify Source Code Analyzer, HP Fortify On Demand, HP WebInspect
IBM Rational	www-01.ibm.com/software/rational/	AppScan Source, AppScan Build, AppScan Tester
Klocwork	www.klocwork.com	Insight
Veracode	www.veracode.com	Veracode SecurityReview

Source: Aberdeen Group, August 2011

Summary: Key Takeaways for Getting Started Now

The *dynamic nature of the application security threat landscape*, the *size and diversity of the typical enterprise application software portfolio*, and the *material financial impact of an actual security-related incident* are among the most visible drivers for increasing investments in application security. Perhaps the most compelling driver, however, is the fact that *all* respondents in Aberdeen's benchmark study experienced a *positive return on their annual investments in application security*. From multiple perspectives, the clear takeaway is that application security initiatives represent extremely good business value – so the most logical thing to do is to **get started**. Best practices include:

- **Adopt a risk-based approach**
  - Identify your application portfolio, to understand the inventory of applications you already have.
  - Identify your greatest risks, to give your highest priority to the specific applications, or classes of applications, which represent the greatest probability of occurrence, frequency of occurrence, and financial impact per occurrence.
  - Identify the specific application vulnerabilities you have, and prioritize remediation based on your use of application security tools in combination with your own experience and judgment.
- **Understand and use the tools at your disposal**
  - Leverage *application vulnerability scanning*, *penetration testing*, *manual source code reviews*, *static source code analysis and verification*, *dynamic source code analysis and verification* as the tools and technologies that most strongly differentiate the companies that achieved the best results.
  - Favor the solution providers that give you maximum flexibility of deployment options, e.g., *on-premise software*, *on-demand solutions*, or subscription-based *software-as-a-service* – along with outside expertise as you need it – as the smartest choices to ensure the success of your initiative.
- **Crawl, Walk then Run – but start with the end in mind**
  - Establish clear ownership and accountability for application security with an executive or team, to help arrive at an acceptable balance between business context, risk-based business judgment, and overall management philosophy on what to address – and when.
  - Start small (e.g., with a proof-of-concept) and then expand by building on your success, in a proven and pragmatic "crawl, walk, run" approach.
  - Partner between the IT Security and Application Development teams, and ultimately establish a common view of where in the software development lifecycle you

feel that application security vulnerabilities are most appropriately identified and remediated.

- Establish well-defined communication channels between IT Security, Operations and Application Development teams, to improve both the efficiency and the effectiveness of identifying and remediating application security vulnerabilities.
- Train the developers on application security policies and best practices – an area where the research shows that virtually all companies can improve.
- Provide your management team with visibility into the application security vulnerabilities and incidents identified and the time and cost to remediate them, so your business leaders will have the information and insights they need to ensure that resource allocation is consistent with strategy.

And as it turns out, taking the right first steps towards implementing best practices in application security provides the potential for even stronger benefits and results down the road. For more information on this or other research topics, please visit www.aberdeen.com.

Related Research	
Secure Remote Access: From the Outside In, to the Inside Out; January 2011	*Securing Your Applications: Three Ways to Play*; August 2010
The State of IT (In)Security, and How to Avoid Costs by Investing More; Dec. 2010	*Web Security in the Cloud*; May 2010
Security and the Software Development Lifecycle: Secure at the Source; Dec. 2010	*IT Security: Balancing Enterprise Risk and Reward*; January 2010
Web Application Firewalls: Defend and Defer; October 2010	*The 2009 PCI DSS and Protecting Cardholder Data Report*; Nov. 2009
Application Scanning and Penetration Testing: Find and Fix (Later); Sept. 2010	*Application Security*; June 2008
HP Acquires Fortify Software, Strengthens Application Security Assurance; Aug. 2010	*Aberdeen Group / IT Security Channel*; complimentary webcasts
	Securing Your Applications; interactive assessment tool (complimentary)

Author: Derek E. Brink, Vice President and Research Fellow, IT Security (Derek.Brink@aberdeen.com)