Gartner

Research

Publication Date: 1 December 2005 **ID Number: G00127407**

Now Is the Time for Security at the Application Level

Theresa Lanowitz

Applications must be available, useful, reliable, scalable and, now more than ever, secure. Therefore, build security directly into the application life cycle to reduce costs and significantly increase application security.

WHAT YOU NEED TO KNOW

Managers of application development and testing organizations must be willing to identify security specialists on their staffs and invest in training, education and processes for their respective teams. They must work with traditional security teams on the operations side to understand what AD and testing can do to alleviate security risks. At this early stage, managers should work with technology providers to understand the needs and requirements for building security into the application, and making security part of the entire life cycle approach. Managers also must assess the AD and testing organizations to determine whether security is strategic or viewed as an afterthought.

STRATEGIC PLANNING ASSUMPTION(S)

By 2009, 80 percent of companies will have suffered an application security incident, and, as a result, will react by creating roles in the AD and testing organizations to ensure that security is handled at the application level (0.7 probability).

ANALYSIS

Today's successful businesses know no boundaries and work seamlessly with customers, systems integrators, virtual teams, offshore providers and trusted partners worldwide. Although firewalls and other security tools can curb most network penetrations, application-specific security tools can only offer limited protection for flawed applications. Reducing software flaws and improving security features (such as authentication) are the most-powerful tools to protect enterprise applications.

Application development (AD) and testing organizations must be proficient in creating, modifying, maintaining and testing applications to deliver security as well as features and functionality. Security at the application level is a nascent area in which developers are poorly trained; however, technology providers are gearing up to assist businesses with the necessary skill growth.

What is application security?

Application security involves developers creating secure source code to prevent the inclusion of a potential security vulnerability, and involves test groups conducting vulnerability testing, application scanning and penetration testing to validate. Some of the most-common problems with source code that increase the risk of a security vulnerability include:

- Buffer overflows
- Error handling
- Command injection
- Unnecessary code
- Malicious code
- Broken threads
- Invalidated parameters
- Cross-site scripting

- Caching, pooling and reuse errors

Application security focuses on three elements:

- Reducing security vulnerabilities and risks
- Improving security features and functions such as authentication, encryption or auditing
- Integrating with the enterprise security infrastructure

Although security represents many things to many people, the application has been primarily focused on features and functionality, and the market drivers are primarily time to market and cost. Security is another facet of quality — and like quality, security must be built *into* the application, not tested at the end of the development cycle.

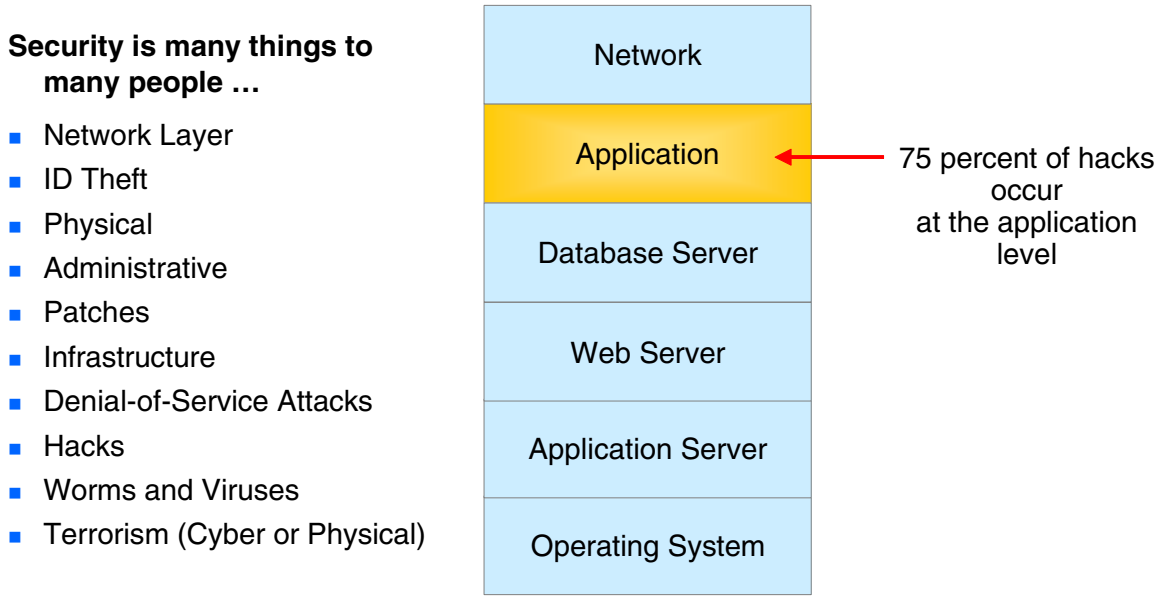
By 2009, 80 percent of companies will have suffered an application security incident, and, as a result, will react by creating roles in the AD and testing organizations to ensure that security is handled at the application level (0.7 probability).

Businesses have always been under threat of reliability and security events due to vulnerable source code. Although application outages are an unwelcome but inevitable event, an application outage caused by or coupled with a security violation is far more disastrous because of the loss of information, the difficulty in system recovery, lost productivity and so on. Part of the plan in building secure software is to make security part of the unified and comprehensive application life cycle. Having security at the start is crucial. Without skilled and trained professionals in the AD and testing groups, businesses won't build in security from the start and, as a result, security incidents will be far more likely.

The "last mile" in terms of security is the application. The best network, host and data security can't effectively protect a weak application. Security must be considered *first* in the application. This translates to planning for security in the application life cycle (see Figure 1). AD and testing (process and application quality) organizations should heed the following action items:

- Develop a security strategy for AD and testing groups.
- Mandate security training for AD and testing staffs.
- Include security reviews in the development process as a codified set of behaviors.
- Perform a security review with the security team before development begins (that is, include the security team as a project stakeholder).
- Build security into project requirements (business and technical).
- Conduct security testing during development and use commercial tools (see "Stay Ahead of Changing Software Vulnerabilities").
- Require sign-off from the security team, just as you would from any other project stakeholder, before application deployment.

Figure 1. Security 101



Source: Gartner (November 2005)

Application Security in AD and Testing Teams

AD and testing organizations are responsible for building applications, and they must understand and implement security for the entire application. Whether it's source code or an executable file, AD and testing organizations must identify where security defects or vulnerabilities are in the application.

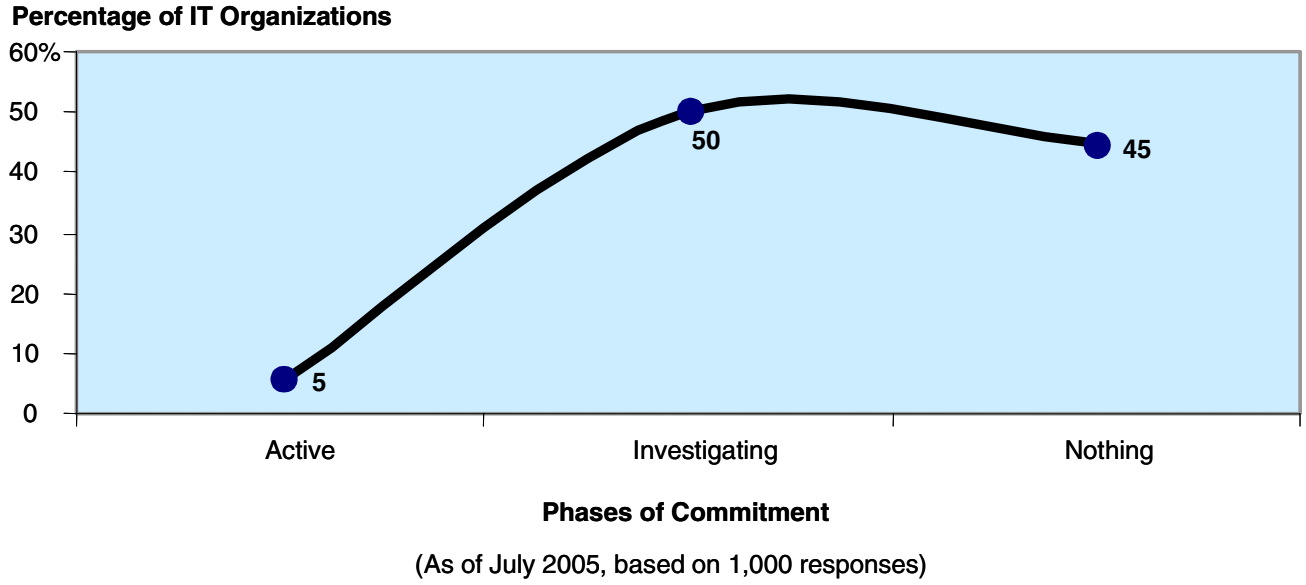
It's been predicted that AD organizations would become extraneous due to outsourcing, the decreasing need to develop custom applications and the lack of technical capabilities. Those predictions have proved false, however, because AD and testing organizations provide significant value to how a business is run. Companies plan to ensure that events resulting from security incidents with applications never occur, and the AD and testing organizations will turn those plans into reality.

AD organizations are still building and maintaining code. Testing organizations are still responsible for process quality and application quality for custom code and packaged applications. AD and testing organizations, whether internal or outsourced, are essential to ensure that software is developed efficiently, effectively and securely.

Security is a new skill that AD and testing organizations must take on immediately. Training for security at the application level will happen on the job. However, few security professionals are proficient in the nuances of development, and few development professionals are proficient in the area of security. AD and testing organizations should invest in outside assistance to meet their application security needs. Outside consulting companies such as Cigital and Security Innovation are examples of professional service providers that have proficiency in the area of application security. Prior to contracting with a professional service provider, AD and testing organizations should obtain references from similar customers, detail the scope of work and understand exactly what deliverables are expected. Professional service providers are likely to already have the much-needed security skills. If the AD and testing organization considers application security to be a strategic investment, then it should also invest in adequately training its AD and testing staffs. Combining on-the-job employee training with professional service providers is a

reasonable way to achieve knowledge transfer. Today, fewer than 5 percent of IT organizations are actively working on application security (see Figure 2).

Figure 2. Application Security Adoption



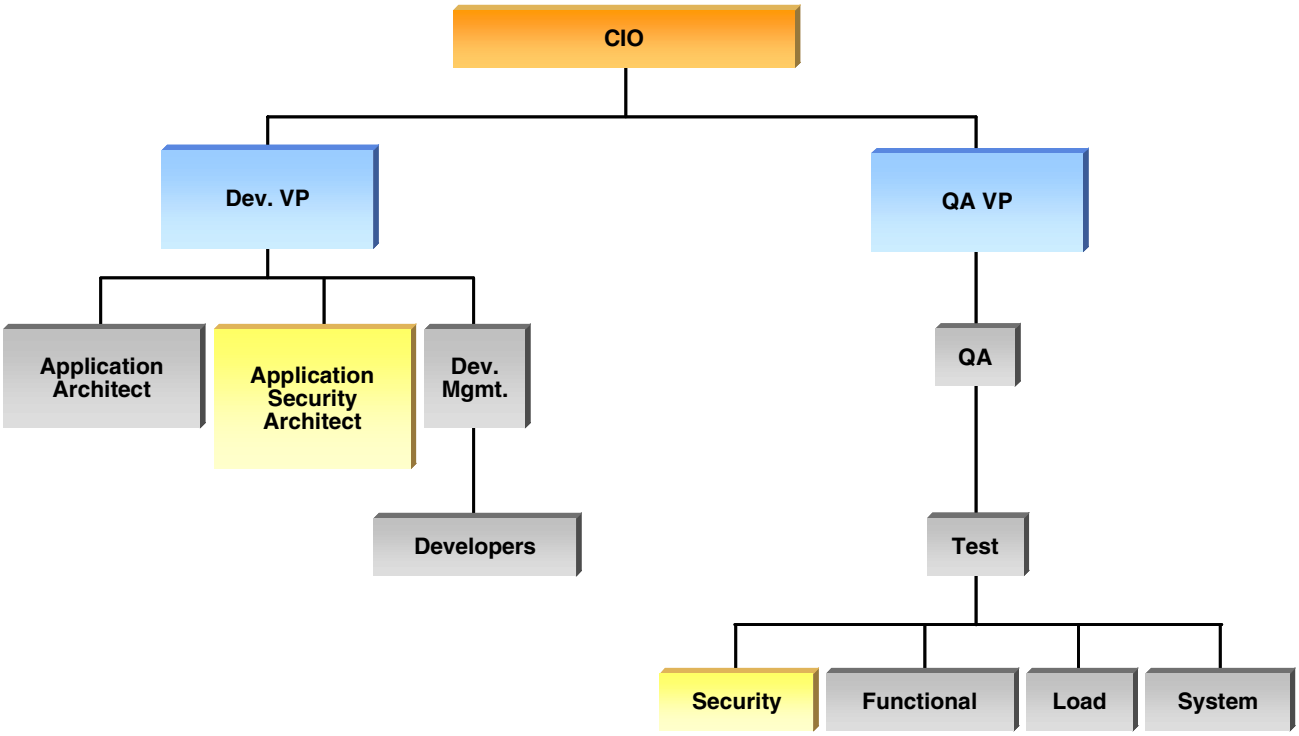
(As of July 2005, based on 1,000 responses)

Source: Gartner (November 2005)

The application has always been a known security threat, but historically it hasn't received the attention required. In today's IT organization, new issues such as compliance, regulations, risk management and ever-changing priorities are increasing the focus on application security. The boundaries between AD and operations, where security has primarily been a factor, must be shattered. Information, plans and requirements regarding security must begin at the application level. Within AD and testing organizations, new roles with improved security skills will emerge.

The application life cycle plays a significant role; it takes the emphasis away from AD (code creation) and places it squarely in the requirements phase. Improving security at the application level starts with the requirements phase. Teams can use popular business "storyboarding" products to build requirements for security, thereby demanding the creation of a test for that particular security requirement. The line of business that establishes the requirements must understand the consequences of failing to address security in the business requirements phase. The ideal scenario would be a consistent set of requirements across most projects, with increased levels of security in special cases. A process must also be built into the life cycle to establish requirements, test compliance and modify the base as new threats, tools or techniques become available (see Figure 3).

Figure 3. A New Level of Awareness



Source: Gartner (November 2005)

Today, developers are focused on building the right things at the right time for their customers. Organizations with a mature line of business will demand security from their applications. For the most part, testing is viewed as something conducted (if time permits) at the end of the development cycle. Because of the focus on time to market and doing more with less, primary test efforts have largely been focused on verifying functionality, not proactively investigating the potential effects of security defects. Tools, although not a panacea, have been focused on automation and productivity, not proactive analysis to prevent security incidents. Testing groups must be aware that security testing should focus on high-fidelity (low false-alarm rate) tests. Approximately 20 percent of application security testing tool rules will find 80 percent of errors with low false-alarm rates. Going beyond that level will cause false positives that will frustrate developers, waste expensive development time and generally result in less security, not more.

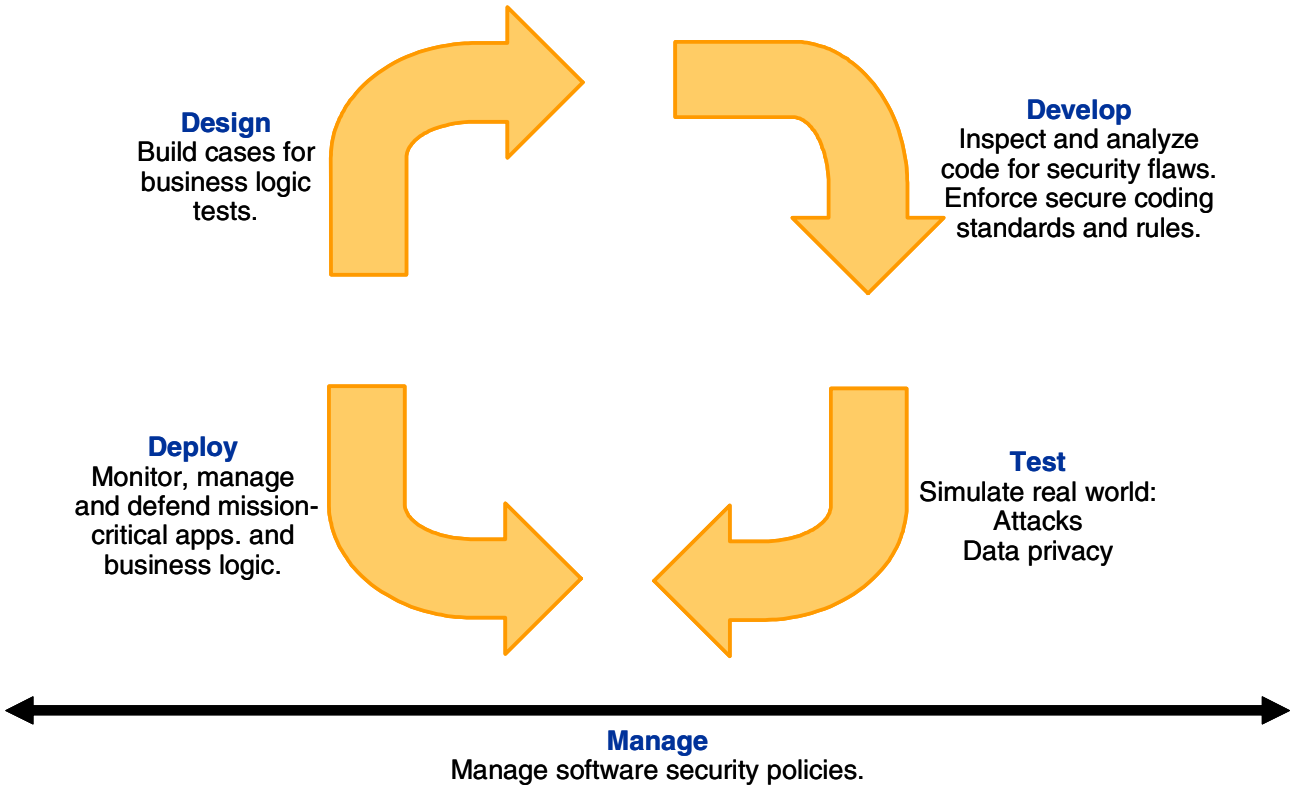
As the U.S. National Institute of Standards and Technology demonstrated in its May 2002 study, "The Economic Impacts of Inadequate Infrastructure for Software Testing," removing a software defect *after* a system is operational can cost two to five times *more* than if the defect was fixed during the final testing phase. This study emphasized that removing those defects during code and unit tests can reduce the cost impact by an additional factor of three to 20. Although defects ideally should be removed as early as the requirements analysis and architectural design phase, Gartner estimates that if 50 percent of software vulnerabilities were removed *prior* to production use for purchased and internally developed software, then enterprise configuration management costs and incident response costs would be reduced by 75 percent each.

The cost of fixing vulnerabilities and regression-testing the repaired code can be reduced by a factor of at least three by detecting security errors during code and unit tests, compared with finding errors during integration tests. Detecting commonly made coding errors during this phase

can also provide feedback to other modules that are still in the design and early-coding phases, so they can avoid repeating the same mistakes.

Throughout the application quality life cycle, risk is continuously assessed. Risk assessment is gaining information about security, performance, application metrics, service-level agreements and more, and turning that information into knowledge. The knowledge gained from ongoing risk analysis becomes the power to understand the application, to identify security vulnerabilities, to understand when an application will begin to degrade, and to stop an application from going into production (see Figure 4).

Figure 4. Security in the Application Life Cycle



Source: Gartner (November 2005)

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner