

# FEW FULLY PREPARED FOR SOFTWARE SECURITY RISKS

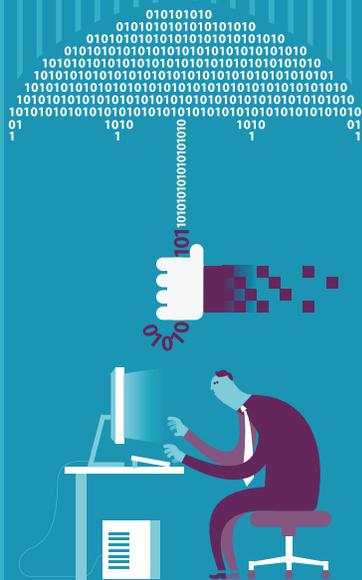


Survey underscores a lack of full-scale software security testing programs.

## Contents

The State of Software Security	2
Little or No Oversight	3
The Value of Building in Security Assurance	4
How Software Security Assurance Works	5

Relatively few enterprises have a full-scale software security testing program in place, despite growing concerns about security issues within the applications their businesses depend on, according to a recent Gatepoint Research survey of IT and security decision makers. Those findings indicate a majority of organizations are at risk that their applications could be used in a manner that causes financial damage, loss of intellectual property, or business interruption, or just will not perform as intended.



Enterprises are critically dependent on software to run business operations, from the back office to customer engagement. In the past, security in software development was an afterthought and coders too often built applications with little attention paid to security. In addition to their own in-house software development issues, many enterprises rely on third-party developed software over which they have little or no insight into software security assurance (SSA) practices.

With cybercriminals constantly probing commercial enterprises to expose security gaps, SSA is an increasingly critical element of security strategies. Yet less than half of the respondents to the Gatepoint survey express confidence in the security of the software that is running their businesses, despite the risks they perceive from potential attacks.

The Gatepoint survey, conducted on behalf of HP Fortify, polled 300 IT and security executives, half of whom are equally divided among financial and business services and the other half are from a wide range of industries including consumer services, education, healthcare, media, and manufacturing. More than three-quarters hold director through CxO positions, and 50% work for Fortune 1000 companies.

### The State of Software Security

Two-thirds of survey responders say their organizations are critically concerned about security issues within their

applications. But while application security has never been more important for enterprises, just 11% of survey respondents indicate they know with confidence what applications are at risk.

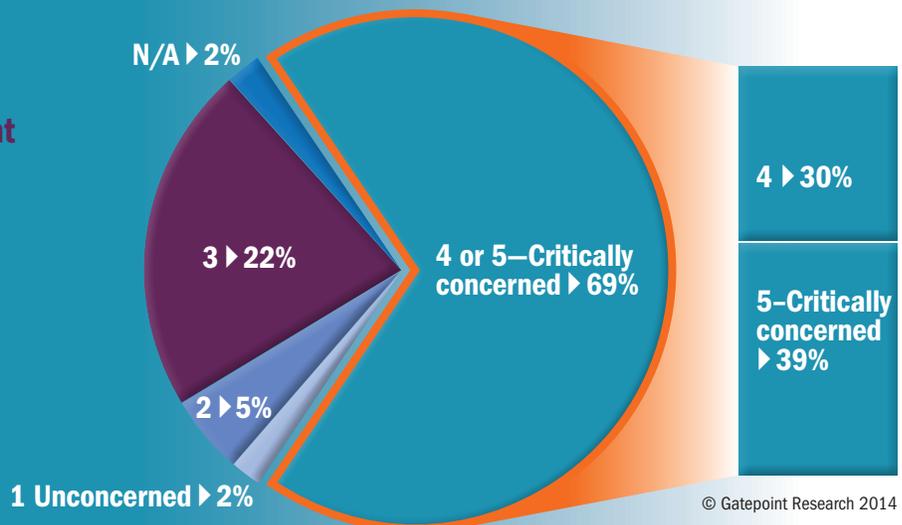
Enterprise software is typically at risk due to insufficient testing and remediation (i.e., removing vulnerabilities), says Bruce C. Jenkins, application security program strategist with HP Fortify. “The primary risk of insufficient testing is overlooking a vulnerability that is a specific threat to an enterprise. If an enterprise is relying on limited penetration testing or if a third party is not well versed in their environment, they could overlook something that is not obvious but could be exploited. That could leave the enterprise wide open to major compromises, data loss, or simply losing control of the IT environment.”

More than half of those polled in the Gatepoint survey indicate they view corporate security under a cloud as cyber attacks increase and become more sophisticated. They have a right to be concerned, according to the results of the Ponemon institute’s *2014 Cost of Cyber Crime Study*, which reported that organizations experienced a 176% increase in the number of cyber attacks, with an average of 138 successful attacks per week, compared to 50 attacks per week when the study was initially conducted in 2010.

Furthermore, according to Ponemon, the average annualized cost of cybercrime incurred by a benchmark sample of U.S. organizations was \$12.7 million, an increase of 9% or \$1.1 million over the average cost reported in 2013.

**An estimated 84% of all security breaches are application-related, not firewall violations. To what extent is your organization focused on addressing security issues in its applications?**

Rate on a scale of 1-5:  
1 = unconcerned, 5 = critically concerned



## Little or No Oversight

Even though most security breaches are software-related, too few organizations employ full-scale software security testing programs. Even if they are confident of their own internal development processes, much of enterprise software is sourced from external providers over which enterprise IT and security staffs have little if any oversight into security assurance—unless external code is subjected to an up-front security analysis, flaws are likely to be exposed only in final testing.

Historically, software has been coded with little or no security “baked in.” As a result, as [Information Security](#) pointed out, “There’s never any respite from the seemingly endless stream of new software vulnerabilities and patches to apply.”

When an organization has to respond to a breach or a new compliance mandate, HP Fortify’s Jenkins says, the response often is to acquire new tools and begin scanning across systems, which can turn up an overwhelming number of faults that need to be fixed. The result is often paralysis: “it’s too much raw data for the security and development teams to analyze, prioritize and make actionable,” he says.

In fact, most organizations have a full plate before even considering remediation issues. Slightly more than half of respondents in the Gatepoint survey say the biggest challenge to achieving software security goals is keeping up with business demands for software deployments.

The next most challenging issue, according to 48% of respondents, is getting various stakeholders to agree on software security goals and procedures.

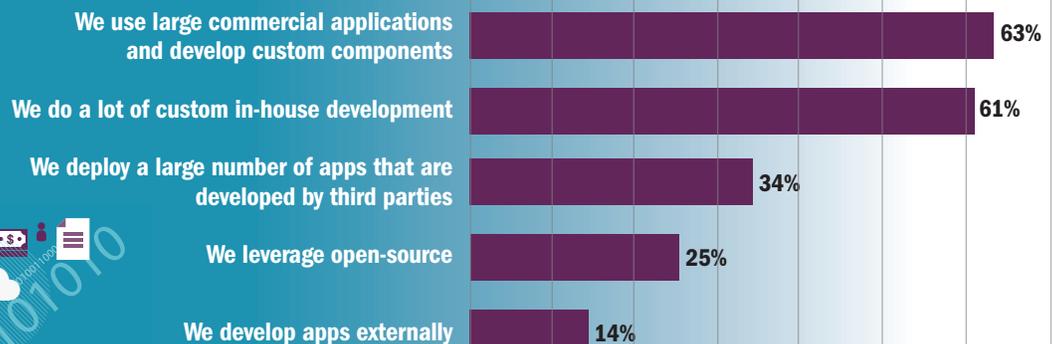
Ownership for the security of software may not always be clear. Typically, an enterprise relies on a diverse portfolio of commercial off-the-shelf, outsourced, and open source applications, in addition to internally developed software.

According to the Gatepoint survey, 63% of respondents say they use large commercial applications and develop custom components; also, 61% do substantial in-house application development. But almost half rely on external development for more than 25% of their applications, and a substantial portion say more than half their portfolio is externally sourced.

“With internal developers you can train them on something the organization perceives to be wrong with its code and how they should address that,” says Jenkins. “But there are very few contracts written today that include provisions allowing the enterprise to mandate certain levels of security that external developers must adhere to.”

As enterprises increasingly turn to Web and mobile applications to enhance usability and agility, they are expanding the potential threat profile and providing cybercriminals with more opportunity to probe for faulty code or information that could be of use to a malicious hacker. The *HP Cyber Risk Report 2013* found that 46%

## How does your organization currently procure, build, and integrate software applications?



of mobile iOS and Android applications use encryption improperly. Furthermore, according to that report, 56% of the applications under test exhibited weaknesses to revealing information about the application, its implementation, or its users, and 31.5% of the applications were prone to leak system information through poor error handling.

### The Value of Building in Security Assurance

Despite the growing risks, just 35% of survey respondents say they have full-scale software security testing programs in place. Most rely on penetration testing (74%) to find software security weaknesses and on perimeter defenses (67%) to stop potential breaches. In essence, applications at risk are lying in wait for an intruder to slip around defenses that have proven time and again to be beatable.

Software security assurance is intended to ensure those risks are never programmed into applications in the first place, or are detected during systematic scanning processes. According to the U.S. government’s [Committee on National Security Systems](#), software assurance “is the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the life cycle.”

Software security assurance comprises best practices and technical solutions to ensure proactive application security. It addresses the problem of software risk within an organization, and assures that software cannot be used in a way that might cause financial damage, loss of intellectual property, or business interruption.

SSA encompasses a preventative approach to software security. It prescribes a set of activities, including comprehensive identification and removal of security vulnerabilities in software and enhancement of an organization’s existing development and software procurement processes.

The most cost-effective and least disruptive way to deal with security vulnerabilities is in the development process. According to the National Institute of Standards and Technology (NIST), after an application is released into production, it costs 30X more to fix than during design. Resolving issues early in the development cycle makes the most economic impact to the business.

According to a study by Mainstay Partners<sup>1</sup>, organizations reduced remediation from one to two weeks to one to two hours, on average, saving \$44,000 per year per application, as a result of introducing automated SSA technology and best practices. Mainstay found that companies realize substantial benefits from SSA right out of the box, saving as much as \$2.4 million per year from a range of efficiency and productivity improvements.

What are you doing to improve security at the application level?





Application vulnerabilities are believed to account for an overwhelming portion of security breaches. Vulnerabilities are built into software code as applications are developed, but developers are not security experts; their task is to take the system and application requirements and distill into code that will solve the problem or accomplish the task at hand. It is essential for an organization to adopt the processes and utilize the tools that ensure code is reviewed, tested, and verified early in the development stages.

HP's Cyber Risk report found that 80% of applications contain vulnerabilities exposed by incorrect configuration, such as server misconfiguration, improper file settings, sample content, outdated software versions, and other items related to insecure deployment. Attackers are significantly escalating their exploitation of Java by simultaneously targeting multiple CVEs and using Java more often to successfully compromise victims' computers. More than 70% of the applications under test fell victim to improper implementation of key security features such as access control, authentication, confidentiality, cryptography, and privilege management.

Acxiom, a data technology company that works to enhance the targeted marketing capabilities of its clients, runs an application security program for static code scanning within its development engineering group. Part of the solution is HP Fortify Static Code Analyzer (SCA), in conjunction with HP Software Security Center (SSC), which makes it possible to find and resolve vulnerabilities early.

"Within your development lifecycle, the closer you get to release, the more expensive and the more time-consuming it becomes to resolve any issues that are found," says Acxiom IT Security Engineer Brenton Witonski. But, he adds, "If you can identify a security issue in the code during the normal development phase and fix it as part of the standard process, the cost is miniscule by comparison."

### How Software Security Assurance Works

Whereas the software quality assurance function assures that an application will perform as it was intended, SSA assures that it cannot be used in a way that might cause financial damage, loss of intellectual property, or business interruption.

SSA is an ongoing, evolving program that encompasses sound software development lifecycle practices, threat intelligence, and ongoing process improvement. Senior management, though, is increasingly aware of the issue, according to survey respondents, half of whom say their companies are beginning to set clear objectives and goals for business software and applications

Application vulnerabilities are believed to account for an overwhelming portion of security breaches. Vulnerabilities are built into software code as applications are developed, but developers are not security experts; their task is to take the system requirements and distill into code a solution that will solve the problem or accomplish the task at hand. It is essential for an organization to adopt the processes and utilize the tools that ensure code is reviewed, tested, and verified early in the development stages.

HP's *Cyber Risk* report found that 80% of applications contain vulnerabilities exposed by incorrect configuration, such as server misconfiguration, improper file settings, sample content, outdated software versions, and other items related to insecure deployment. Attackers are significantly escalating their exploitation of Java by simultaneously targeting multiple CVEs and using Java more often to successfully compromise victims' computers. More than 70% of the applications under test fell victim to improper implementation of key security features such as authentication, access control, confidentiality, cryptography, and privilege management.

Jenkins advises organizations to avoid being overwhelmed by the totality of the effort and to start with security objectives that will support the enterprise's mission and key business goals. "For example, if I'm in the financial sector and one of my goals is to protect customer data, I can develop a strategy to do that and set out some other goals, such as identify all the critical risks within our top 10 Web-facing applications. From there you can establish time-constrained, measurable objectives."

Jenkins says that even organizations that are not able to obtain budget for SSA initiatives can take advantage of training recommendations, best practices, and even some testing components, from organizations such as the [Open Web Application Security Project \(OWASP\)](#). HP now offers a managed application security testing service that enables organizations to quickly test the application security of a few applications or launch a comprehensive security program without additional investment in software and personnel.

Once grounded in basic SSA practices, organizations can increase their capabilities by investing in static analysis solutions that provide feedback to developers early in the lifecycle and dynamic analysis during the testing, Q/A, or preproduction phases. By starting with secure coding guidelines and performing code vulnerability assessments regularly, the enterprise will improve its development practices and embed ongoing application risk assessments.

"The approach we've taken is one of 'Discover early, resolve early,'" says Paul Phillips, head of Software Assurance and Integration at British Gas. "We try to engage with projects right at the beginning of the lifecycle, in the concept phase, so we understand what the project is looking to deliver. Then we have a number of core service offerings, with static and dynamic scanning being two key aspects of that. We work out a plan and the appropriate funding that allows that project to deliver secure code. We're trying to make sure that project deadlines are not impacted by discovering a big lump of vulnerabilities right at the end of the development lifecycle."

Software security is a serious and growing problem. To mitigate the risks, enterprises must ensure their software development organizations start thinking about security as a part of every step in the total software development life cycle. For more info, visit [www.hp.com/go/fortifyssa](http://www.hp.com/go/fortifyssa).

"Does Application Security Pay? Measuring the Business Impact of Software Security Assurance Solutions," 2013. Mainstay.

### How does senior management regard application security?

