

WORLD QUALITY REPORT

2015-16

SEVENTH EDITION



Security Testing is the Top IT Strategy Priority

Multiple Platforms Increase Risk

Yves Le Floch, Vice President, Head of Business Development, Cybersecurity TLI, *Sogeti*

Industry reports suggest some 80% of security breaches occur at the application layer, while 86% of web applications have issues involving authentication, access control, and confidentiality. This stark reality undoubtedly sits behind the strategic importance of security identified in this year's World Quality Report. In terms of IT strategy, security scores most highly with a ranking of 6.2 on a scale of 1 to 7. This is ahead of even customer experience (6.1) and IT cost optimization (6.1), which are understandably high scorers. Just one industry – Transportation – fails to place security in its top three priorities.

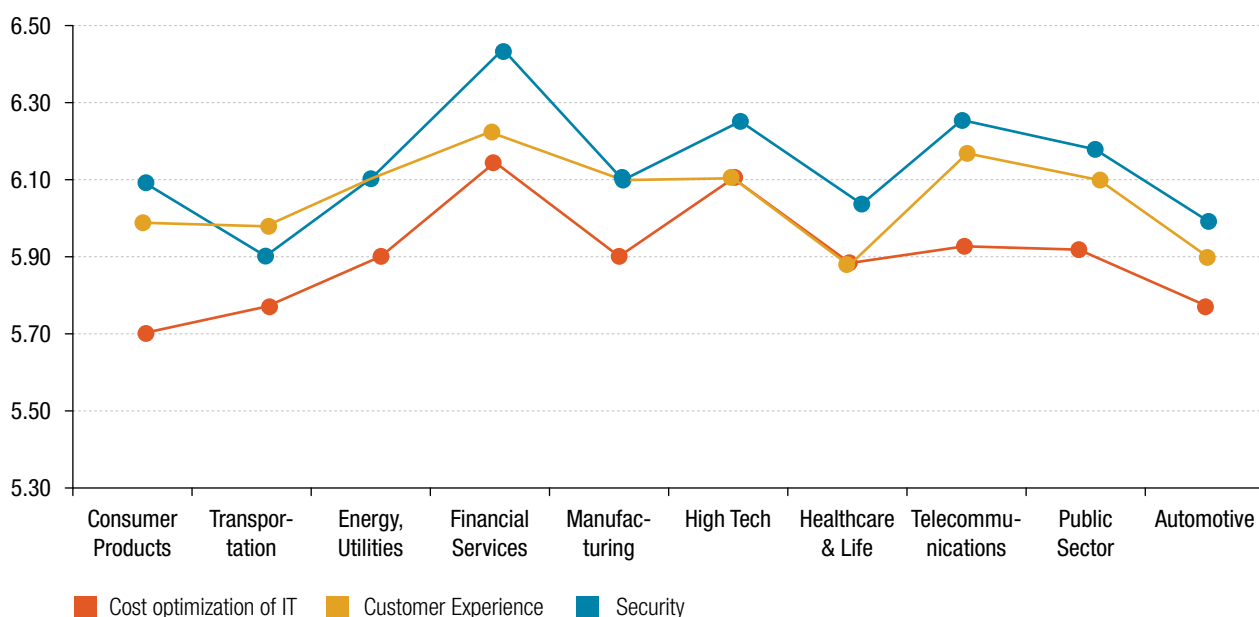
At a geographic level, security is the number one IT strategy priority in all but two regions, the Nordics and South East Asia, which place customer experience first.

The heightened awareness of security is driven by Digital Transformation, which increases the number of vulnerable touch points, and drives mobile access and data proliferation. An average 80% of our survey respondents (85% in Financial Services) say security is important or very important.

Until recently, the security of applications was viewed as low risk because they were largely internal, so securing the infrastructure was sufficient as a priority for protecting against security risks. But IT solutions are no longer contained in isolated environments. Web-based, mobile and cloud-based applications capture and hold sensitive corporate and customer data, and are accessible from multiple platforms. However, they are highly vulnerable to intrusion, hacking, etc. Despite this increased vulnerability, the pressure to release

Focus areas for IT Strategy

FIGURE 13



quickly often means the security checks needed to manage applications and systems in depth are incomplete.

Lack of security in this complex digital IT landscape has significant ramifications for the business, notably in terms of the potential for financial loss, competitive disadvantage, and reputational damage if a security breach becomes public. It is proven a high number of people will leave or avoid companies

that have had security issues. It is no surprise, therefore, that security testing has become a business imperative for many organizations. Indeed, this year's World Quality Report survey data reveals that protecting the corporate image is ranked as the single most important objective for QA and Testing. In the light of the huge damage to the corporate image that a data breach can cause, security testing is a critical component in Digital Transformations.

Healthcare and High Tech top the tables for systematic security

Responses to the survey reveal that 46% of participating organizations are systematically performing security testing on every application release. Despite security being the highest priority, nearly 25% are failing to systematically perform security tests on all applications, preferring to limit this activity to critical ones only.

There is considerable divergence in the amount of systematic security testing across different industries. The Healthcare (88%) and High Tech (85%) sectors stand out as the biggest users of systematic security testing. At the lower end of

the spectrum, but still with a high priority rating, the Public Sector (57%) performs the least amount of systematic security testing.

The survey reveals a similar divergence geographically, although not as dramatic in terms of percentage. Leading the pack in systematic security testing are UK and Ireland (89%), South East Asia (85%) and North America (83%). At the other end of the scale, although again at a fairly high level, are Western Europe (68%), Southern Europe (63%) and Australia and New Zealand (62%).



We are in a financial services industry; the data that we have is personal, and any leak of data would be bad for business and our customers. There is an extremely strong emphasis around security, both internal as well as the external.

VP,
Financial Services, North America

Increased automation enables security testers to do more with less

It is far less costly to remove a critical vulnerability before a service goes live than after it has been launched (or breached). Thus the primary function of application security testing is to identify and fix vulnerabilities early during the software development lifecycle in order to reduce costs, improve efficiency, and enhance application security. Automated security testing is playing an increasingly important role in this.

The 2015 research data reveals the steady progress of automation in the wider testing of applications, with 45% of all

test cases now automated. There is still a high dependency on manual work, however, when it comes to security testing. For example 52% of the organizations perform manual code review as part of their security testing activities. This has both cost and resource ramifications, with the physical line-by-line code checking to identify anything that might produce vulnerabilities in production being slow, costly and labor intensive. Test coverage is also a challenge with manual testing, something that automation addresses.

Add to this the concerns about the availability of skilled testers in some regions, especially a scarcity of security specialists, and the only practical approach is to move to more automated, or partly automated, security testing as the way ahead. This automation is already taking hold in many places with a number of different types of automated security testing being used, such as dynamic application security testing and static application security testing. There are several tools available for this, either proprietary or commercially available, and we are seeing an increase in the use of such tools.

More than half (57%) of respondents perform dynamic security testing, where security testing is performed by actively running security test cases against the application to uncover vulnerabilities. This is the most used security testing approach today, and is designed to find those vulnerabilities most prone to exploitation. It takes place later in the development lifecycle, just before code is released in production. In combination with penetration testing, which is performed on the application in a live production environment, (currently used by only 39% of respondents), dynamic security testing is a powerful security test solution.

Penetration testing adds another layer of security testing, in that it goes beyond just applications to try and exploit infrastructure vulnerabilities. The 39% figure shows that structural penetration testing still has room to grow within most organizations.

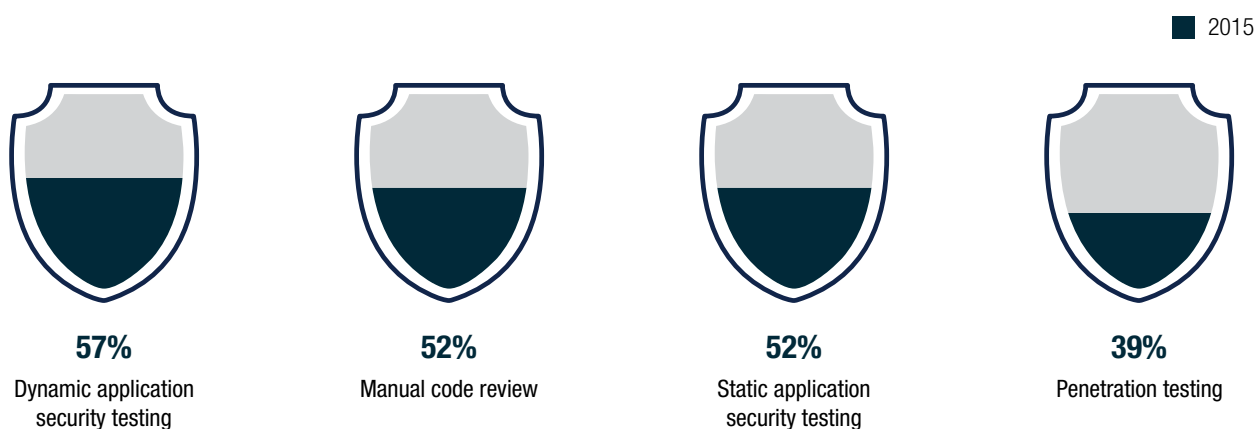
Static security testing is used by more than half of the organizations interviewed, scoring 52%. It is typically performed by development teams using scanning tools to check code as it is written. Static security testing finds many more vulnerabilities than dynamic testing, but not all of these will be exploitable. Taking place earlier in the development lifecycle— during the development phase — static security testing is a valuable approach for reducing the cost of application development because of the well-known principle that the sooner an issue is identified, the less it will cost to fix.

The right approach to security testing will require a solid combination of manual test activities by security specialists and automated security checks and tests. For maximum benefit organizations should combine automated testing, which is typically comprehensive, repeatable and scalable, with manual testing focusing on the areas that can't be tested automatically.

In the security testing space, the increase in automation is helping to identify vulnerabilities at different stages in the development lifecycle, from requirements definition onwards. Up to 44% of the participating organizations carry out application security assurance activities during requirements definition although, as outlined below, there is still greater use of security testing at the later stages.

Commonly performed security testing activities

FIGURE 14



Mixed approach to how security testing is conducted

There is a mix of approaches to performing security testing, comprising internal, external, and managed services provision. It is a function requiring specialist security skills and some organizations prefer to use their own internal specialists due to the commercial sensitivity of what is being tested. In other cases, the unique role that security testing has in wider testing activities, and its incidental nature, make it an area of testing that will benefit from external security specialist support. External providers bring deep experience of security issues across multiple organizations and sectors. The World Quality Report research found both internal and external experts being used to perform security testing, along with a range of technologies and engagement models.

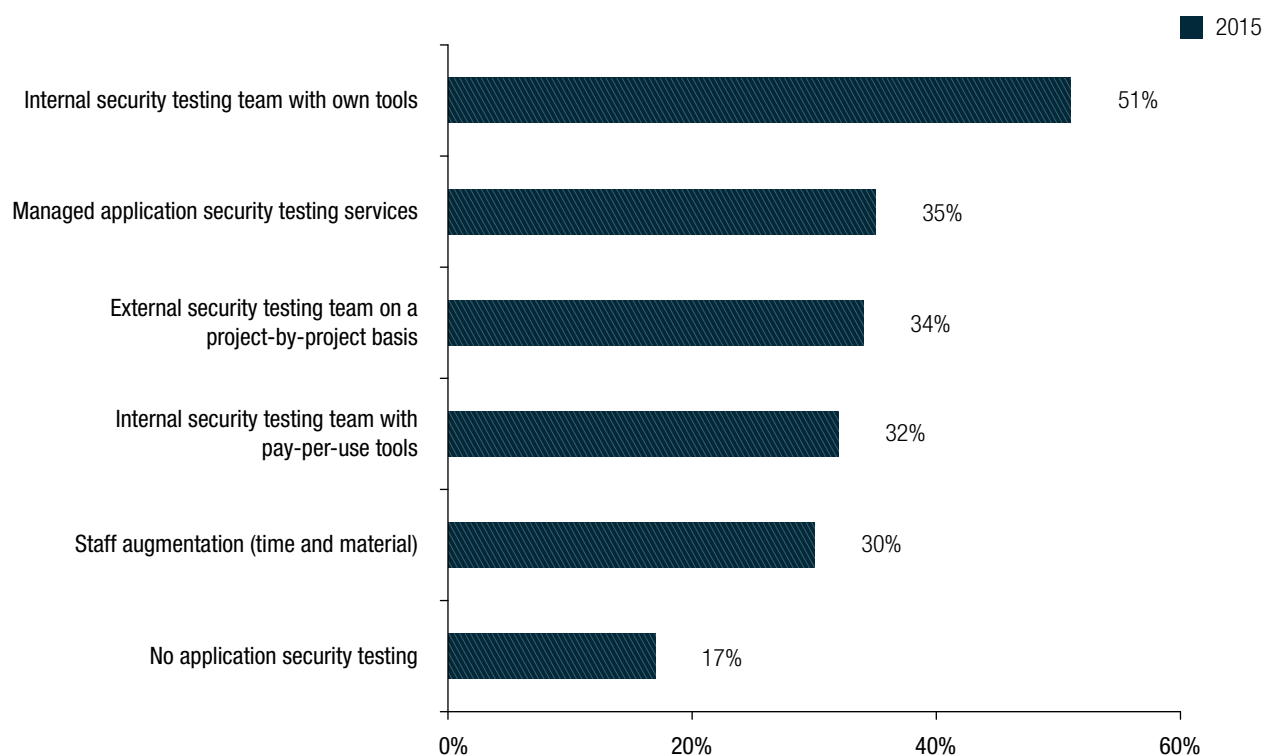
At a global level, the findings can be broken down as: 51% use internal experts with own tools; 32% use internal specialists with pay-per-use tools; 35% use external managed security test services; 34% use external security experts on a project-by-project basis; and 30% use external

security test staff augmentation. There are large geographic differences, however, with South East Asia notable for its use of a fairly even combination of internal and external resourcing. Interestingly, three industries in particular use more managed services than other approaches: High Tech, Financial Services, and Automotive.

The importance of security is indicated by the investment in internal security teams, with over half of organizations using them. However, there is the risk that internal teams might have less exposure to or experience of new security issues and therefore miss certain security checks. Speed of release and volume present internal teams with a big challenge because reliance wholly on in-house specialists limits the scalability and reactivity needed for this highly specialized test approach. Further investment in security and automated security testing, in combination with some form of external application testing support, can help to mitigate this risk.

Type of security testing team

FIGURE 15



Last stage application development is where most QA and security testing is performed

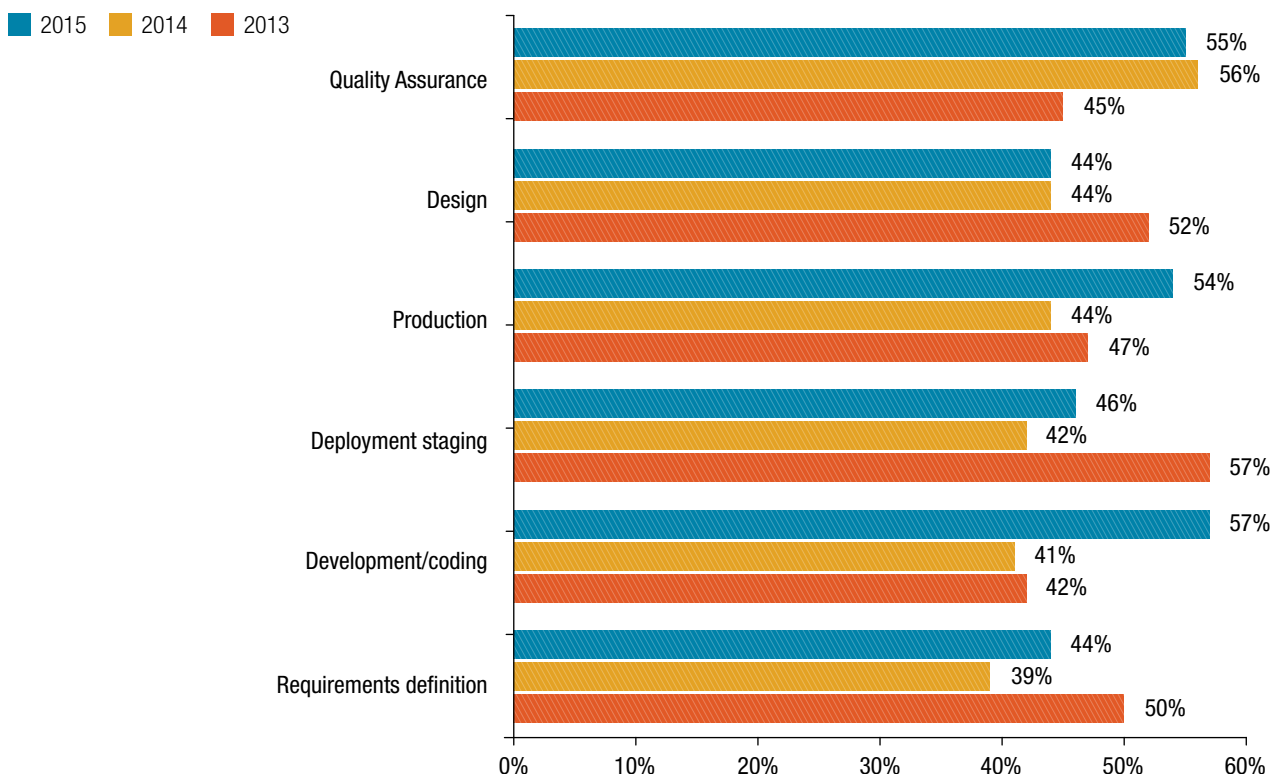
Where in the application development lifecycle should application security testing take place to reduce risk? For organizations participating in the World Quality Report 2015 study, it appears to be later, rather than sooner in the lifecycle, as indicated by the greater use of dynamic application security testing discussed earlier. In general, however, there is increased attention being paid to security testing in all phases of the application lifecycle.

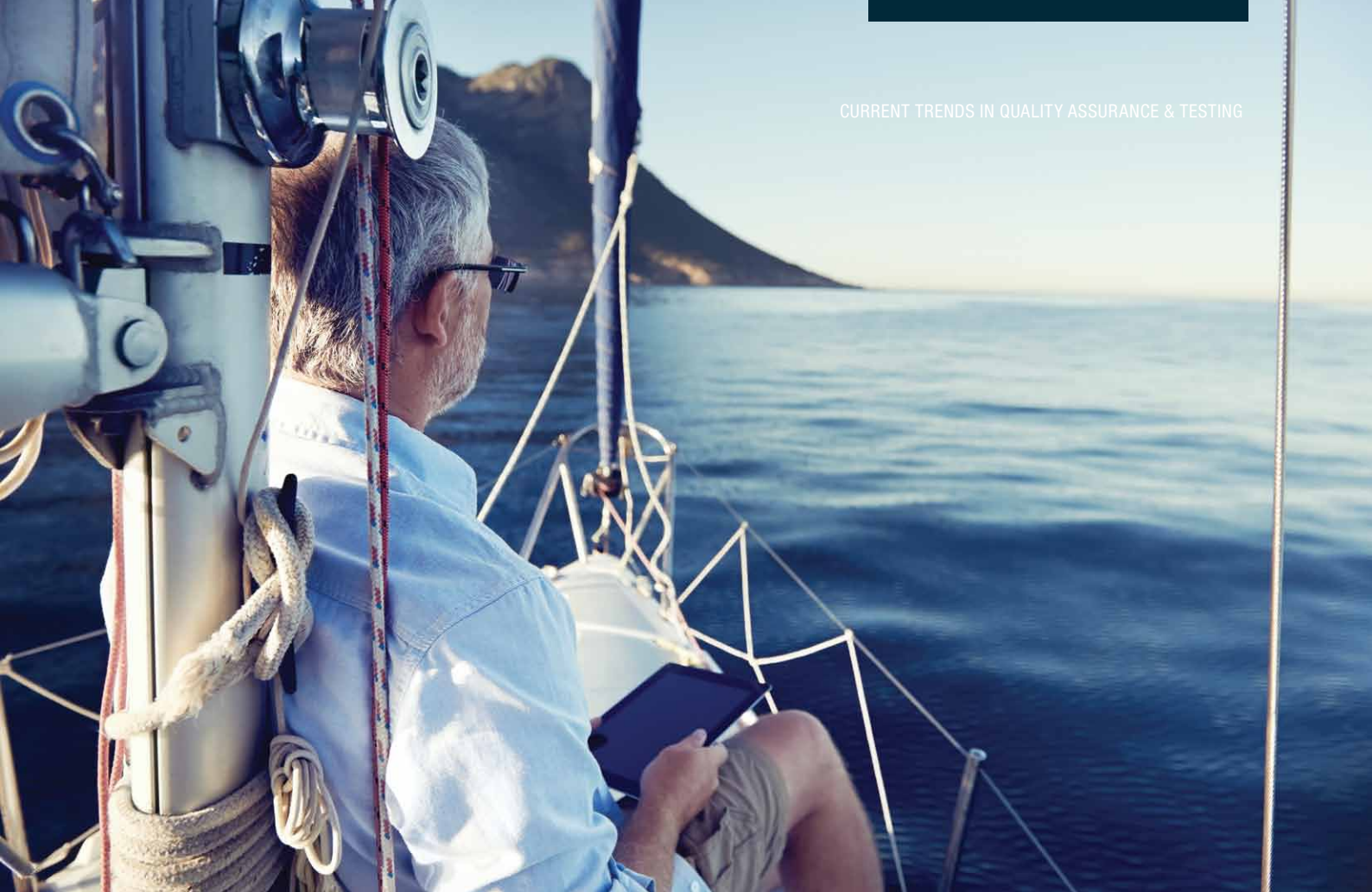
More than half (57%) perform security testing in the development/coding phase, with the Financial Services, Telecom and Automotive sectors giving this phase their highest ranking. This is a big increase from last year's 41% at this lifecycle stage. Security testing is performed the least during requirements and design phases (44%), while 55% of respondents perform security testing during their QA, a marginal 1% drop over last year.

There are different lifecycle stages at which organizations undertake application security assurance activities. Some will focus more on requirements during early stages, while others concentrate more on testing during later stages. The attention being paid to security QA has increased in almost all phases of the application development lifecycle. The development/coding phase shows the fastest increase, which is understandable because this signals the increase of static code analysis and dynamic security testing (for which one needs to have the developed code available). Also the increase in the production phase is notable, and this is a signal that organizations are paying more attention to security monitoring and penetration testing of applications in production. It is encouraging that attention to security has also increased in the requirements phase. However, the focus on security in the design phase is still at the same level as last year. As security QA matures further, we expect to see a greater level of focus on security aspects in this phase.

Top 3 Aspects for IT Strategy for security testing across Industries

FIGURE 16





Looking ahead for security testing

The rate at which today's fast-paced world continues to release new applications designed to enhance the user experience is speeding up. Cloud-based testing in general is on the increase, but security testing in or from the Cloud is approached with more caution in certain regions. For example, there is a big difference between North America (46%) and Western Europe (33%) performing security testing in a cloud-based environment. Where caution does exist, issues of trust, of massive surveillance and high profile security breaches have resonated, slowing the uptake of security testing in a cloud-based environment. Security is the biggest area of focus for testing mobile applications (55% of respondents that do mobile testing), ahead of scalability and performance testing (54%). The proliferation of mobile devices and applications, with their inherent security challenges around control of access points and device security, means this looks set to remain a trend for the future.

Looking ahead, the findings from this year's World Quality Report study will make interesting comparisons in the coming years. Many organizations feel that there is not enough time to spend on testing digital applications (social, mobile, Cloud, Internet of Things) due to the pace at which they are released and this increases the risk to their critical

business applications. This is also likely to shape the future approach to application security testing with higher levels of automation and industrialization.

The use of external security testing services, either on a project-by-project basis or as managed services, is becoming more established and will alleviate the pressure on often costly and hard to retain internal talent. The focus for internal security expertise should be on hiring key senior level personnel, such as a Chief Security Officer to advise the executive on application security and testing. Handing off the day-to-day work, or increasing automation, will enable more application development projects to reach the production stage, faster, safer, and with more scalability.

While more permanent relationships with external security testing providers are desired, security testing has not yet reached that level of maturity in many cases. Certainly, with 54% of respondents saying they do not perform systematic application security testing on every release of every application, despite security being the number one strategic IT priority, too many organizations are exposing themselves to major application security risk. This is something to watch out for in the future.

About the Sponsors

About Capgemini and Sogeti

With almost 180,000 people in over 40 countries, we are one of the world's foremost providers of consulting, technology and outsourcing services. The Capgemini Group reported 2014 global revenues of EUR 10.573 billion. A multicultural organization through and through, we've developed our own way of working via the Collaborative Business Experience™ and Rightshore®, our worldwide delivery model.

Sogeti is a leading provider of technology and software testing, specializing in Application, Infrastructure and Engineering Services. Sogeti brings together more than 20,000 professionals in 15 countries and has a strong local presence in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Cap Gemini S.A., listed on the Paris Stock Exchange.

Together Capgemini and Sogeti have developed innovative, business-driven quality assurance (QA) and Testing services, combining best-in-class testing methodologies (TMap® and TPI®) to help organizations achieve their testing and QA goals. The Capgemini Group has created one of the largest dedicated testing practices in the world, with over 17200 test professionals.

Learn more about us at:

www.capgemini.com/testing or

www.sogeti.com/testing

About HP

HP is a technology company that operates in more than 170 countries around the world. We explore how technology and services can help people and companies address their problems and challenges, and realize their possibilities, aspirations and dreams. We apply new thinking and ideas to create more simple, valuable and trusted experiences with technology, continuously improving the way our customers live and work.

No other company offers as complete a technology product portfolio as HP. We provide infrastructure and business offerings that span from handheld devices to some of the world's most powerful supercomputer installations.

More information about HP (NYSE: HPQ) is available at www.hp.com

Thank you

Capgemini, Sogeti and HP would like to thank

- The 1,560 IT executives who took part in the research study this year for their time and contribution to the report. In accordance with the UK Market Research Society (MRS) Code of Conduct (under which this survey was carried out) the identity of the participants in the research study and their responses remain confidential and are not available to the sponsors.
- All the business leaders and subject matter experts who provided valuable insight into their respective areas of expertise and market experience, including the authors of country and industry sections and subject-matter experts from Capgemini, Sogeti and HP. Some of these

Main Report Authors

Mark Buenen and Ajay Walgude

Writer (Main Report)

Ngaire Mckeown

Assistant Writer (Region/Country Pullouts)

Archit Revandkar

Program Manager

Mitali Kini

Creative Design

Partha Karmakar

contributors and their area of contribution are: Vincent Groener for testing budget trends, Philip Borsen and Sathish Natarajan for test automation, Shiva Jayaraman for Digital, Deepika Mamnani for agile and DevOps, Renu Rajani and Shiva Balasubramanian for test environment management & test data management, David Harper (HP) and Anantharaman Iyer for security testing and Max Tau for CPRD.

- Hilary Croft, Parvathy Nair and the Marketing & Communications Offshore Services (MCOS) team for their support in the production of this year's report.

Partner Management

Jean-Philippe Favrot (HP), Karthik Ranganathan, Satish Varghese, Mary Johnson, Julia Mulcrone

Market Research

Stephen Saw and Ian Parkes (Coleman Parkes Research)*

Printing and Distribution

Annie Bates and David Cole (Crucial Colour)

*Ian Parkes, CEO and co-founder of Coleman Parkes Research, is a full member of the Market Research Society. All research carried out by Coleman Parkes Research is conducted in compliance with the Code of Conduct and guidelines set out by the MRS in the UK, as well as the legal obligations under the Data Protection Act 1998.

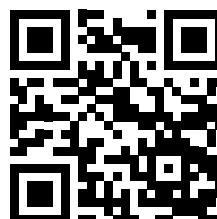
www.worldqualityreport.com

©2015 Capgemini, Sogeti and HP. All Rights Reserved.

Capgemini and HP, and their respective marks and logos used herein, are trademarks or registered trademarks of their respective companies. All other company, product and service names mentioned are the trademarks of their respective owners and are used herein with no intention

of trademark infringement. Rightshore® is a trademark belonging to Capgemini. TMap®, TMap NEXT®, TPI® and TPI NEXT® are registered trademarks of Sogeti, part of the Capgemini Group.

No part of this document may be reproduced or copied in any form or by any means without written permission from Capgemini and HP.



Testing Global Service Line, Capgemini Group

Govind Muthukrishnan

Senior Vice President, Leader, Testing GSL
govindarajan.muthukrishnan@capgemini.com

Mark Buenen

Vice President, Global Solutions Lead, Testing GSL
mark.buenen@sogeti.com

Capgemini Application Services

Ajay Walgude

Vice President, Solutions Lead
Financial Services GBU
ajay.walgude@capgemini.com

Anand Moorthy

Vice President, Global Testing Leader
Financial Services GBU
anand.moorthy@capgemini.com

Julian Clarke

Principal, Testing Leader
julian.clarke@capgemini.com

Sathish Natarajan

Service Delivery Director, Testing Leader
sathish.n@capgemini.com

Sogeti

Brian Shea

Chief Executive Officer, UK
brian.shea@sogeti.com

Shiva Jayaraman

Service Delivery Director,
Global Testing Transformation & Large Deals Head
shiva.jayaraman@capgemini.com

Yves Le Floch

Vice President, Head of Business Development,
Cybersecurity TLI
yves.le-floch@sogeti.com

HP

Jean-Philippe (JP) Favrot

Global Alliance Director
jp.favrot@hp.com

John Jeremiah

Technology Evangelist,
HP SW ADM Digital Research Team Leader
john.jeremiah@hp.com