# WORLD QUALITY REPORT

SECURITY ANALYSIS 2014-15 SIXTH EDITION

# CYBERSECURITY

Application security testing is integral to the wider enterprise application testing environment

The sixth edition of the *World Quality Report* from Capgemini, Sogeti and HP revealed valuable insights into application security relating to global testing practices. In particular, the report highlights the impact of SMACT (Social, Mobile, Analytics, Cloud and Internet of Things) technologies on the modern testing landscape. The following document is based on data collected from more than 1,500 enterprises participating in the 2014 WQR survey. They were drawn from private and public sector organizations ranging in size from 1,000 employees to more than 10,000.

## SECURING DIGITAL TRANSFORMATION

With digital transformation on the agenda, SMACT (Social, Mobile, Analytics, Cloud and Internet of Things) technologies are having an impact on the modern testing landscape. Notably, digital transformation has increased awareness among senior business and IT executives of the significance of Quality Assurance (QA) and Testing. Application security testing is a key component of this.

The increasing focus on enhancing the user experience through the rapid release of new applications poses a very real risk. This rapid release cycle and new SMACT technologies create new vulnerabilities for IT systems. The *World Quality Report 2014-15* points to the frequent need for organizations to maintain the critical balance between velocity and quality, while adapting to digital change. Quality is a leading indicator of loyalty and brand equity. This is driving a change in focus areas for QA and Testing teams:

- QA and Testing are increasingly involved in transformational projects, for which security is a top focus.

One of the emerging trends in global testing practices is the increasing importance of mobile testing – and the role of security within this. Organizations are spending 17% of their testing budgets on mobility. Mobility is all about the user; It gives customers, employees and other stakeholders anytime, anywhere access to applications and systems. With a much reduced tolerance on the part of users for application errors, security or performance issues, it is no wonder that security is a big focus in mobility testing:

- 54% of the mobile testing focus is on security.

The pressure on organizations to release new mobile applications at speed is a concern. Some 40% of respondents say that they don't have enough time to test their mobile solutions, yet it is essential to systematically test all web and mobile applications before release, particularly if they are highly regulated, including the security aspect.

New digital transformation projects and the adoption of innovative IT technologies are also changing the types of skills required from the testing organization, and these are often costly or hard to find. There is a lean towards more technically able resources, including experienced security testers. Failure to invest sufficiently in application security puts enterprise assets and data at risk. This is perhaps one of the reasons organizations are extending their in-house testing capability by engaging with external service providers, including security testing providers, in a co-managed approach:

- 70% of organisations now engage with external service providers, up from 49% in 2012.

Download the *World Quality Report 2014-15* at www.worldqualityreport.com

## Securing the user experience

Application security in the digital enterprise goes beyond purely fighting cybercrime, although that in itself is a growing issue. Organizations must be able to confidently operate and engage with customers in new ways, using SMACT technologies and always-on applications. The *World Quality Report 2014-15* therefore recommends a focus on all-channel experience testing for validating the end-to-end customer experience. It describes the validation of application security as a 'critical step' in this, alongside a combination of functionality, ease-of-use and performance testing.

CONTACT

**Yves Le Floch**
VP, Head of Development for Cybersecurity, Sogeti
yves.le-floch@sogeti.com

**Claire Souhaut**
Enterprise Security Products Director, HP France
claire.souhaut@hp.com

Security testing is a non-functional testing activity, whether carried out jointly with a testing partner or in-house. The *World Quality Report 2014-15* recommends investing in state-of-the-art security testing, with services comprised of identifying security requirements, threat analysis, static security code evaluation, and dynamic security vulnerability testing.

The report adds that it is essential to pay special attention to identifying risks for unauthorized intrusion at the application, network, and data and storage levels. Security services should provide testing support for any type of application, from new cloud and mobile initiatives to existing legacy applications. Furthermore, flexibility in the delivery model is one way of managing the cost of application security:

- Security testing is a good candidate for a Testing as a Service model that can be provided at a fixed usage or output-based price.

## SECURITY IN THE CLOUD

There is an unmistakable trend toward the adoption of cloud-based testing:

- Executives taking part in the *World Quality Report 2014-15* survey predicted that nearly half (49%) of all applications could be validated using cloud technologies by 2017.

Security is a vital aspect of this evolution. It currently holds the top spot in the key areas of focus for testing migration projects:

- 59% of respondents pay special attention to data security, requirements and risk when testing application migration to the cloud.

As more and more organizations migrate to cloud-based solutions for their test environments, security can also be a deciding factor in the type of cloud adopted. Some organizations prefer to adopt a private cloud with its inherent security, control and ownership; others are more open to a public cloud where speed of deployment, as well as reduced maintenance and operating costs, are deciding factors. We can see this most markedly in the healthcare and public sectors, both of which are governed by strict data privacy requirements: Only 25% healthcare and 26% of public sector applications are hosted in the cloud, as opposed to 34% among high tech companies. In the slower adopting healthcare and public sector organizations, adoption is mostly by way of private, tightly controlled cloud infrastructure. Organizations moving their production environment to the cloud should put in place robust Service Level Agreements (SLAs) with their providers. These SLAs will ensure the providers commit to the highest levels of service in the event of a security breach.

## PUTTING SECURITY AT THE HEART OF TESTING

With 80% of cyber attacks occurring at the application layer[1], the increasing global focus on application security testing is wholly understandable. The pressure to release quickly means that the security checks needed to manage applications and systems in depth are often not completed, whether through a lack of time or limited security resources. As our latest findings reveal, organizations are more and more aware that this leaves them open to attack. To counter this they are embedding security alongside performance, functionality, and customer experience testing as it becomes an intrinsic part of the wider testing landscape.

In an era of social media and instant communications, every application failure poses a risk to an organization's reputation, customer relationships and, potentially, revenue. Application security testing is thus a strategic priority for safeguarding any application and, in an increasingly cloud-based world, from anywhere.

1 Gartner 2014

Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING

SOGETI