QUOCIRCA INSIGHT REPORT

October 2008

Winning outsourcing strategies

How to increase value and reduce risk

Contacts:

Fran Howarth
Quocirca Ltd
Tel +31 35 691 1311
fran.howarth@quocirca.com

Bob Tarzey
Quocirca Ltd
Tel +44 1753 855794
bob.tarzey@quocirca.com

Outsourcing is a strategy increasingly being used by organisations to reduce costs and increase value. Outsourcing, however, has its risks. As organisations look to push out more of their custom software application development needs to outsourcing partners, careful planning is required in terms of building stringent software security requirements into contracts and creating a process and metrics to ensure that those requirements are met. This report examines outsourcing practices from 200 of the largest organisations in the UK and the US and provides pointers as to how the most experienced outsourcers are putting in place effective processes to drive the risk out of outsourcing.

- **Inexperience and a lack of process leads to ineffective outsourcing**
  Industries with the least history of outsourcing experience the most difficulties in successful project completion, while those industries with a long track record exhibit the most satisfaction and success from their outsourcing programmes. While the majority of projects undertaken in the more experienced retail and public sector industries result in success (77.5% and 65% respectively), those undertaken by transport and financial sector companies, where outsourcing is less common, exhibit daunting levels of failure. For example, in these industries, around 50% of projects have been called off completely and 30% of projects undertaken by finance firms have led to legal action being taken.
- **The importance of getting the contract right cannot be stressed enough**
  Those organisations with the most experience stipulate the most stringent functional and security requirements in the outsourcing contract, giving them greater control, helping to reduce the risks of sub-par applications being delivered, and greatly reducing the likelihood of the need for legal action. For example, the most experienced outsourcers (those outsourcing more than three-quarters of their development needs) are three times more likely to stipulate software security audit requirements in contracts than those outsourcing in a more ad hoc fashion.
- **Building in requirements for the use of appropriate security tools and requiring extensive testing against agreed standard methodologies further reduces risk**
  Auditing delivered source code against stated security requirements prior to acceptance through the use of automated code analysis is a recommended best practice for firms that outsource their application development. Among leaders in the retail and public sectors, 62.5% check code with automated code scanners, compared to just 32.5% of finance firms, which outsource the least of all. Such scanners reduce the risk of vulnerabilities considerably. Further, just 40% of finance firms test their applications for the most common vulnerability—cross-site scripting—compared to 82.5% of retailers. This could leave financial organisations' applications at serious risk of attack.
- **Using external providers for application delivery is also outsourcing**
  Security is also important to reduce risk in these fast-emerging delivery models. However, just 47.5% of finance firms mandate that there are controls over who handles their data, compared to 70% in the public sector and 72.5% of retailers, and only 37.5% of finance firms demand any certification of their service providers, compared to 82.5% in public sector and retail organisations.

Conclusion

As demonstrated in this report, successful outsourcing of the creation of critical custom software requires an approach taking into account appropriate levels of rigour. Organisations with lower levels of experience in defining security and process controls should adopt those best practices currently in use by those with more familiarity and success. They can then use these as repeatable practices for ensuring the success of future projects.

RESEARCH NOTE:
The information presented in this report was derived from 200 interviews with those in charge of outsourcing software application development in the UK and the US, and was completed in September 2008.

Respondents were from the very largest organisations that are doing significant amounts of outsourcing in the financial services, public sector, retail, transport sectors, and other large enterprises.

CONTENTS

1. Introduction

With today's tenuous economy forcing organisations to cut costs, whilst at the same time increasing the value that they gain from efficient, secure business practices, one key area in which they can increase the value of their offerings is in developing specialised software applications or services that supplement the more general capabilities of commercial off-the-shelf packaged applications. Such custom applications can add value in numerous ways, such as allowing greater collaboration with business partners, or improving the efficiency of specific billing systems. This is leading to continued rapid growth in the proportion of software applications used by organisations that are developed as one-off projects.

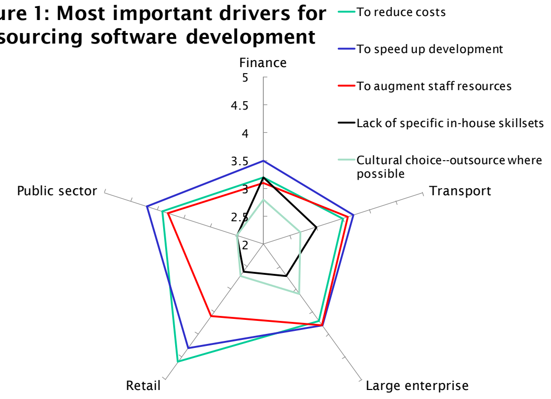
However, maintaining a large application development and testing staff is costly and requires that specialist resources be hired and retained. Because of this, more and more organisations are choosing to outsource the development of software applications to specialist third parties that have experienced resources available, and can use their expertise to develop applications faster and, generally, at lower overall cost. However, outsourcing is not without risk and requires careful planning and control to ensure that projects run smoothly and fulfil the requirements set.

This report aims to show how 200 of the very largest organisations in their industries in the UK and the US that are outsourcing significant parts of their software applications development needs are handling their outsourcing projects. Based on interviews with those in charge of the outsourcing projects, this research aims to uncover the processes that they put in place to ensure that outsourced software application projects deliver value, and how they drive risk out of the projects. Further to this, questions were asked about other fast-emerging forms of outsourcing, including cloud computing and Software as a Service (SaaS). In many of these cases, the main focus will be on the writing of code that acts as "glue" between existing or hosted services, or in the creation of functional components, rather than an entire application being written from scratch. This means that security is an issue that must be considered in these situations also.

2. Drivers for outsourcing

As Figure 1 shows, the primary drivers for outsourcing software application development across all respondents are to speed up the development of projects and to reduce the costs involved, followed by the need to augment staff resources through access to the specialist resources that are available through outsourcers. Also, as comparison with Figure 2 shows, these factors are a key consideration among those that outsource the most—rather than doing projects in a piecemeal fashion where specific skill sets are not available for developing a certain application. This is something that financial services organisations, in particular, could learn from.

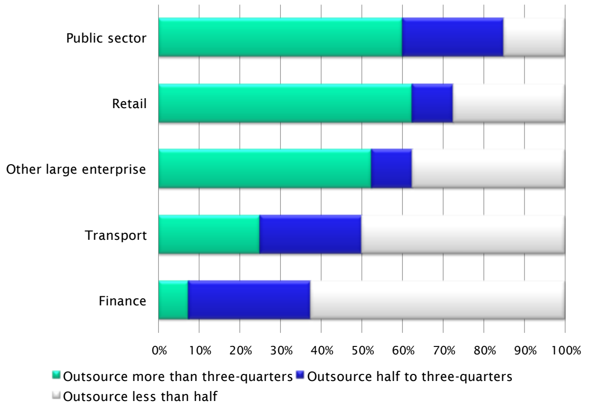
Figure 1: Most important drivers for outsourcing software development



Ranked from 1 = least important to 5 = most important

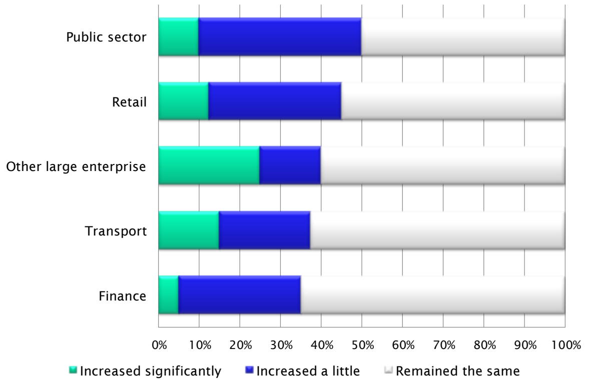
However, some industries have been faster than others to embrace outsourcing as a means of adding value and reducing costs across their application portfolios. As Figure 2 shows, the use of outsourcing for software development is currently greatest among public sector and retail organisations, whilst transport and financial services organisations are comparative laggards.

Figure 2: Outsourcing by industry



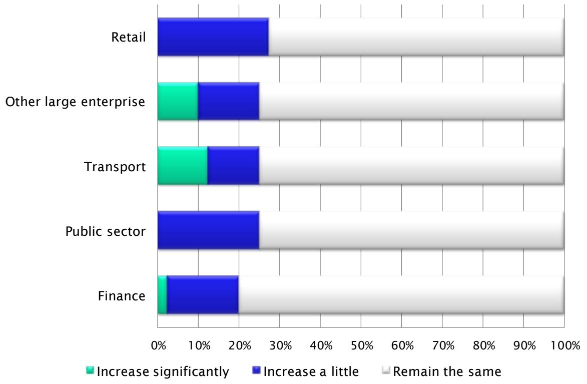
As Figure 3 illustrates, those industries that are leading, in terms of the level of outsourcing they are undertaking, have seen the greatest growth in outsourcing over the past couple of years. This is also borne out by qualitative insights from interviewees, a significant number of which among those outsourcing more than three-quarters of their application development projects indicated during their interviews that they had recently made the move to outsourcing 100% of their software development needs.

Figure 3: Has outsourcing increased over the past two years?



Over the next couple of years, the level of outsourcing is still expected to expand, as Figure 4 illustrates. Although the level of increase is likely to be lower than previously, at least 20% of respondents in every industry will see increased outsourcing activity.

Figure 4: Will outsourcing increase over the next two years?



3. Outsourcing can be a risky strategy

With any outsourcing project, an organisation must place its trust in the hands of its chosen partner. This means that the organisation must trust that secure coding best practices have been followed and that applications have been developed with adequate levels of security built into them—for example, ensuring that a programmer cannot have placed a backdoor into an application that could allow them to access that application after it has been delivered, which could lead to them carrying out a security exploit. However, as Figure 5 shows, organisations are outsourcing even those applications that are used to process and transmit the most sensitive data, such as financial and human resources applications.

Figure 5: Which applications do you outsource development of?

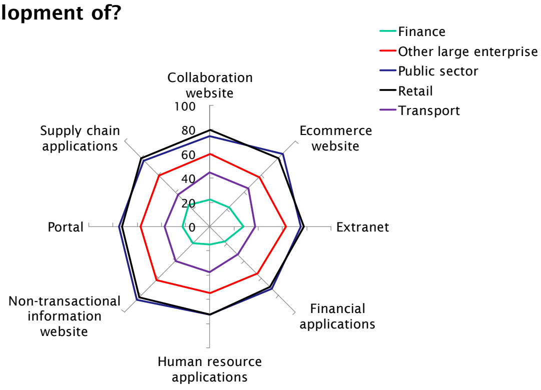
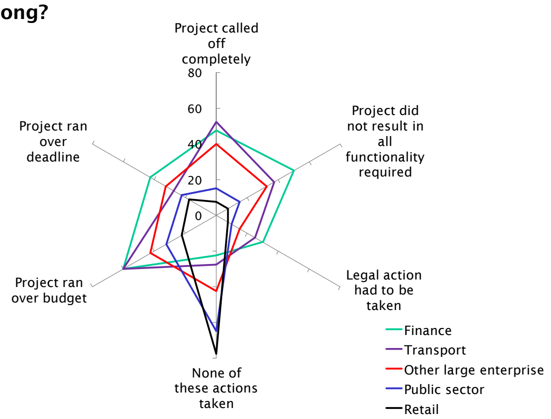


Figure 5 also shows that it is organisations in those industries that outsource the most significant percentage of the application development needs that fully outsource the most sensitive applications—and yet these are the very ones who will encounter the fewest issues with their outsourcing projects. Among public sector and retail organisations, respondents are confident enough to fully outsource development of any type of application included in the chart whilst, in the financial services sector, just 17.5% are happy to fully outsource the development of financial applications.

Does this mean that those that are outsourcing the most are putting themselves at greatest risk? On the contrary; throughout this research, answers to questions indicated that those organisations that are outsourcing the highest proportion of their application development needs are putting in place the tightest safeguards—in terms of requirements set out in contracts, in defining what security tools and procedures should be used, and in the level of testing of applications that they are demanding of their outsourcers. This provides them with the confidence that they need to trust their outsourcers with even the most business-critical software applications.

As Figure 6 indicates, their trust in their outsourcers appears to be well founded. Having taken the trouble to clearly define requirements upfront, respondents from those industries in which outsourcing is most prevalent have encountered fewer problems with outsourcing projects going wrong. For example, just 22.5% of financial services organisations report that they have experienced no problems with outsourced application development projects, compared to 77.5% of retailers. Conversely, 30% of financial services organisations have had to take legal action against an outsourcer as a result of a failed project, compared to just 7.5% of retailers. In total, 17.5% of projects resulted in legal action being taken but, as may be expected, organisations in the US took legal action in twice as many cases as their counterparts in the UK.

Figure 6: Do outsourcing projects ever go wrong?



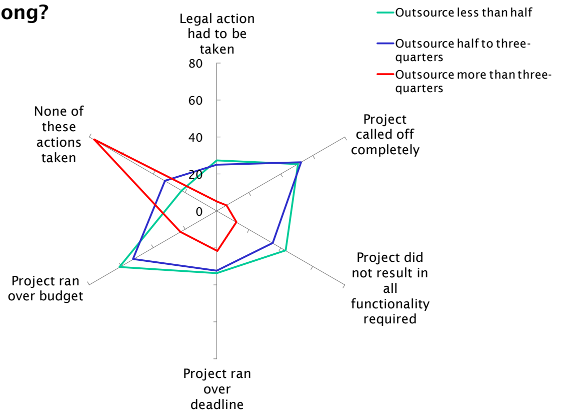
Overall, projects running over budget are the most common problem, experienced by a full 43.5% of respondents, rising to 61% of those outsourcing less than half of their application development needs. As well as this, 32.5% of all respondents reported that projects had been called off completely owing to problems—rising to 46% in the US.

Yet Quocirca does not believe that the types of project being outsourced are inherently different—retailers are dealing with the financial details of customers, just as financial institutions are. The supply chains of retailers are far more complex than those of finance, and the transaction volumes are generally higher. Therefore, project complexity does not seem to be a factor in this.

The fact that legal action has been taken in some cases demonstrates that there was a problem with the outsourcing contract drawn up—giving the organisation nothing to fall back on when problems occurred in terms of an agreed-upon resolution and escalation route. Outsourcing contracts must contain specific requirements detailing vulnerability measures, remediation cost recovery, and specific thresholds for acceptable risk, in order to protect organisations from potential harm. This is especially important for those organisations with the least experience of outsourcing, in order to avoid the creation of overly complex, one-off contracts that could contain loopholes which could be exploited should the dispute need to be settled in court. For example, by defining acceptance criteria that include a list of specific critical vulnerabilities, vulnerability classes, or that mandate a maximum vulnerability risk level, the organisation can describe the conditions that will result in the application being rejected and returned to the outsourcer for remediation. By doing this, an organisation protects itself against the most common threats to its software and systems, giving it legal recourse should the outsourcer refuse to fix those vulnerabilities. In addition, requiring artefacts that attest to the application's security level puts the onus on the outsourcer to either engage a security certification clearing house or automated source code analysis tool to provide reliable information. These best practices, stipulated up front, reduce the likelihood of legal action greatly.

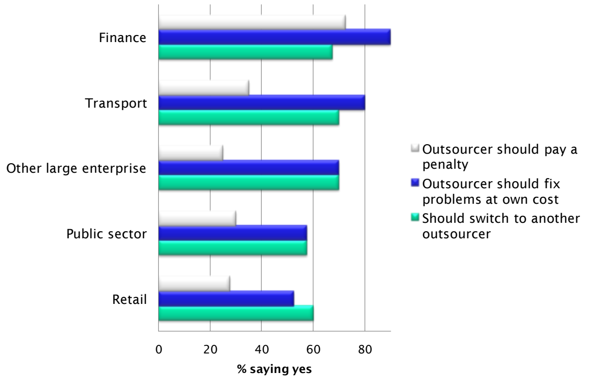
Figure 7 takes a different slant on the same data—comparing problems experienced with outsourced development projects by the level of outsourcing undertaken. This clearly shows that outsourcing does not need to be considered as a risk—so long as the correct processes are put in place. It would seem that experience matters.

Figure 7: Do outsourcing projects ever go wrong?



As Figure 8 shows, this has ramifications for outsourcing providers themselves. If any project should not go according to plan, those organisations with the least experience of outsourcing are likely to impose the stiffest penalties, adding to the costs involved in a project for an outsourcer and reducing their profitability. Such "stick with little carrot" contracts do not tend to work in reality—a contract that majors on how resolutions are to be reached between the two parties will always be a better bet. Therefore, it is in the best interests of outsourcing organisations, and not just the companies that are outsourcing the business to them, to ensure that best practices are followed in clearly laying out exactly what the requirements are at the start of the project. This is especially true for new customers, but also for new projects with existing clients, where contracts developed previously can more easily be repurposed.

Figure 8: If something goes wrong, what is an appropriate response?



In addition to this, the fact that more than 50% of all respondents would move to another outsourcer clearly shows the risk of project failure for outsourcing providers. This would indicate that levels of loyalty are low and do not necessarily translate to repeat engagements. In order to engender loyalty and differentiate themselves, outsourcing providers should chase a mix of best overall value coupled with special deals to attract and retain customers. Part of this could be done through additional differentiation, such as adherence to ISO standards for code testing to provide a layer of assurance that the provider follows best practices.

4. The importance of getting the contract right

Prior to the start of any outsourcing project, it is essential that organisations take time upfront to define their requirements for the application to be developed, including determining how business critical it is and what levels of safeguards need to be built in to ensure that the application delivered is secure. These requirements will form the basis of any contract and will be reinforced through any service level agreement put in place.

When taken across the board, respondents to this survey gave mixed results when stating what they considered to be the essential goals that should be built into the contract. The main exception was for requirements related to staff at the outsourcing partner, for which most were in agreement that stringent requirements should be defined. Among those outsourcing less than half or half to three-quarters of their application development needs, fewer than 20%

of respondents in each category defined the other requirements mentioned as essential. However, far more consistency and emphasis was seen from the "guru" group (those outsourcing more than three-quarters of their application development needs). Since this group has been shown to suffer the fewest problems and rarely experiences project failure, it can be inferred that Table 1 shows the best practices that should be adopted in any code outsourcing project.

Table 1: What baseline goals need to be included in the outsourcing contract	*% respondents outsourcing more than 3/4*
Level of experience required of programmers	75
Skillsets required of programmers	75
Certifications required of programmers	74
Background checks of outsourcer's employees	72
Define level of exposure of application and intended audience	69
Define criticality of applications in terms of revenue gains expected	67
Define internal costs incurred if application failed to function	65
Define goals and metrics for security	64
Develop a risk management framework	60
Establish baseline security needs	56
Roles and responsibilities of all individuals at each party	43

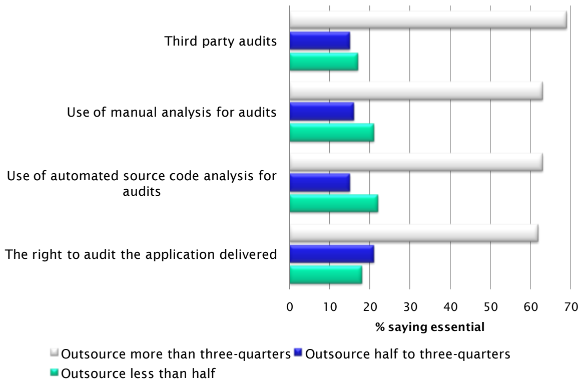
No less critical than identifying the baseline goals of the software and the required experience of the developers, organisations must also define what requirements they have related to application security and the use of security tools and techniques in the development of software applications by outsourcers. These processes should then be written into the contract to provide remediation assurances should the security of applications fail to live up to the standards set. Again, fewer than 20% of respondents outsourcing less than half or half to three-quarters of their application development needs are taking the trouble to define these requirements and to specify the standards needed in the contract. For this reason, the best practices related to application development and security requirements that should be built into outsourcing projects (Table 2) are drawn from those in the "guru" group—those with the most experience of outsourcing of application development.

However, it should be pointed out that attestation that secure coding best practices were followed, while important, is by itself not enough. What is actually needed is some level of certification that such practices were followed, including detailed results that prove this. There are many ways of testing applications that will give repeatable, reliable metrics for this, including the use of source code analysis, penetration testing and manual code review.

Table 2: Application development and security requirements to be included in outsourcing contracts	*% respondents outsourcing more than 3/4*
Level of flaws considered acceptable/unacceptable	78
Remediation processes for serious vulnerabilities	74
Use of user acceptance tests	70
Secure coding practices required, including attestation that followed	68
Logging of all activity during development process	65
Use of automated security code scanning	64
Use of agile software development methodology	61
Use of integrated threat modelling throughout engagement	61
Warranty that includes an obligation to pay for insecure code	57
Warranty that includes no obligation for paying for insecure code	48
Demand strong authentication for all developers	43
Use source code management system for access control	39
Demand segregation of duties enforced by authentication	34

In order to ensure that requirements have been followed, organisations should not only ensure that applications delivered are audited, but also should specify how they require this to be done in the outsourcing contract for each project. However, a similar pattern emerges here in that those for whom outsourcing is not a clear strategy are paying only lip service to these needs (Figure 9). This places them in a poor position in terms of verifying that the applications will perform as required, without serious security vulnerabilities present. It also increases the risk for these organisations that applications will fail to perform as they should.

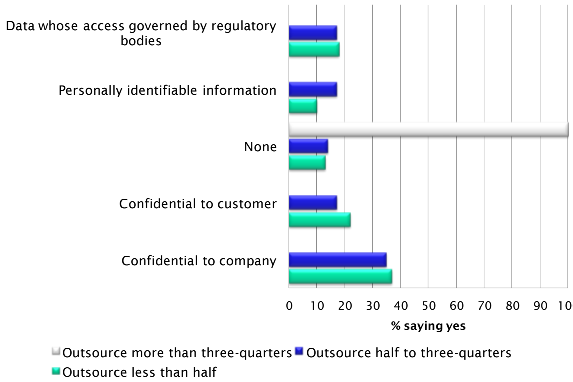
Figure 9: Audit requirements stipulated in the outsourcing contract



Not only is the risk increased that their organisation could be compromised by a security attack against weaknesses in software applications, but it is also likely that costs will be increased as such flaws ultimately cost more to put right. Should the flaw not be caught early and result in a security breach that is brought into the public domain, this could have a further detrimental impact in terms of the organisation's brand reputation and profile.

The efforts taken by those in the "guru" group can be seen in Figure 10. By building stringent requirements into contracts and enforcing standards through service level agreements and data handling procedures, those outsourcing the most do not need to worry about the level of control handed over to outsourcing partners in terms of what types of data they are comfortable with outsourcers handling, as Figure 10 shows. This can be done by detailing such requirements as encryption for data at rest and in motion, unacceptable vulnerabilities and/or vulnerability classes, and the use of synthetic and anonymised data for testing purposes.

Figure 10: Data outsourcers restricted from handling by level of outsourcing



Obviously, agreements have to be in place to ensure that the outsourcing company adheres to the legal requirements for handling any data provided to them—in accordance with the laws that organisations, as their customers, are party to. Therefore, the outsourcing company must understand and be able to demonstrate adherence and compliance to such areas as data protection, data leak prevention, and so on.

Having taken the trouble to define what is required in the contract, no respondents in the "guru" group feel that handing confidential information over to outsourcing partners is a risk as the appropriate safeguards have been built into the contracts. This demonstrates a solid trust relationship between such organisations and the outsourcing companies—something that both sides must strive to maintain. One breach of process or security from either side breaks the relationship too easily and, as the research shows, with loyalty being low within the code outsourcing market, organisations can easily decide to go elsewhere.

5. Reducing risk through use of appropriate security tools

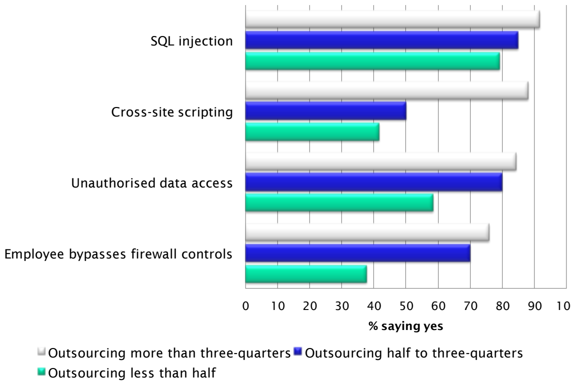
As well as specifying requirements in the contract for an outsourcing project, organisations must define processes for the tools and techniques that they require their outsourcer's development staff to use. The organisation must also ensure that applications are thoroughly tested for security before those applications are delivered. Table 3 outlines the most important tools and techniques that should be used by outsourcing partners in developing software applications, again according to those in the "guru" group. However, in stark contrast to the answers to questions regarding contract development, there is much greater equality being seen among all respondents in the use of security tools and techniques.

Whilst this means that they are taking secure development processes seriously, the use of these tools and techniques should be contractually required—not just be expected.

Table 3: Security tools and techniques outsourcers are required to use	*% respondents outsourcing more than 3/4*
Database layer abstraction	79
Input validation	79
Server configuration	79
Proxies	78
Web application firewalls	74
Data encryption	68
Operating system hardening	67
Source code vulnerability scanners must be used	61
Certification of code used from libraries	59
Certification of commercial off-the-shelf components	58
Certification of open source code used	55

Not all vulnerabilities are of the same risk to an organisation. It is the responsibility of the organisation to prioritise vulnerability types as to the risk they pose the organisation. This then defines the most critical vulnerabilities that must not be present in code in order to reduce risk to their organisation. Again, there is greater equality here amongst organisations according to their level of outsourcing, but those in the "guru" group are still outperforming the rest (Figure 11).

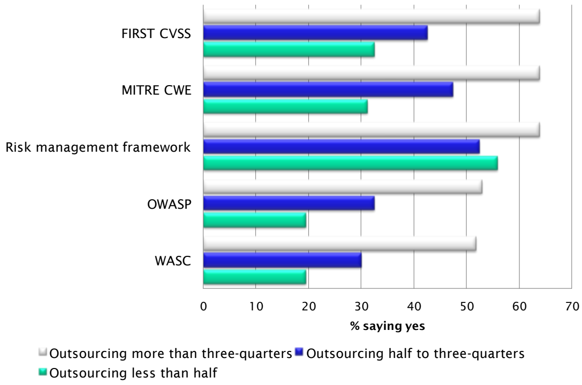
Figure 11: Must outsourcers ensure these vulnerabilities cannot occur?



The vulnerabilities shown in Figure 11 are some of the most common and are considered to be amongst the most critical in terms of security. However, each application developed is different and its design and components could lead to a vulnerability not generally considered to be a serious risk in most situations leading to severe problems owing to the configuration of particular code.

New vulnerabilities, attack methods and vectors also become known at various points during the lifetime of an application, and the outsourcer must be able to demonstrate that they can deal with this. To gauge the level of risk posed by each type of vulnerability according to how it could affect a particular application, risk-rating systems can be used to determine how serious any flaws encountered are, incorporating the level of risk that an organisation would face should those vulnerabilities be exploited (Figure 12). This provides an automated way of proving that the most severe vulnerabilities are not present in applications before they are accepted and put into use.

Figure 12: What risk-ratings systems do you require outsourcers to use?

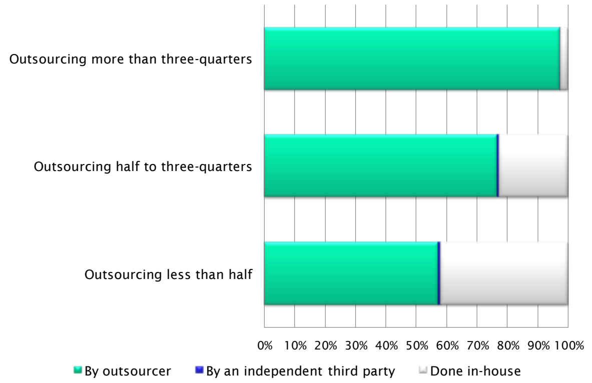


6. Testing applications for security

Since security should be a key criterion for acceptance of a software application developed by an outsourcer, organisations must require that initial security testing is done by outsourcers. This should not, however, absolve organisations from the need to test the security themselves or to have independent validations done. For one thing, this denies an outsourcing provider the chance to claim that the application was signed off by the organisation to which it is delivered in the case of dispute. As shown in Figure 9, above, it is considered best practice to write into the contract that the organisation has the right to audit the application before acceptance.

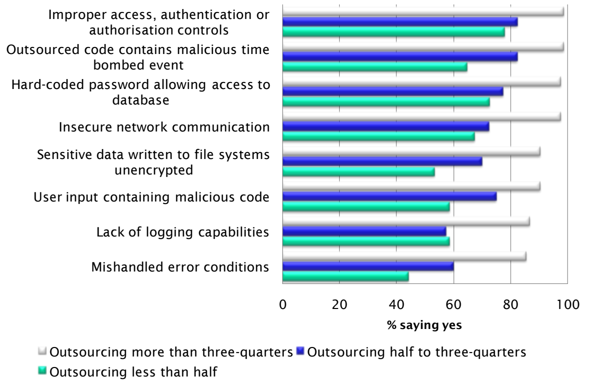
As Figure 13 shows, requiring outsourcers to perform initial testing is a best practice that is not lost on the most experienced outsourcers. Those still developing their outsourcing programmes would do well to emulate this, since performing tests in-house is a more expensive option and requires that the organisation has sufficient qualified resources to conduct those tests. As a general rule of thumb, testing in general, not just for security, eats up around 25% to 30% of an application development project in terms of time, resources required and cost of testing.

Figure 13: How are applications tested for security?



Organisations outsourcing the development of software applications should also define the most serious errors for which the outsourcer should ensure that tests are conducted. As Figure 14 shows, this is a requirement set among the majority of organisations, although the "guru" group still performs the best, reducing overall risk of failure of applications delivered.

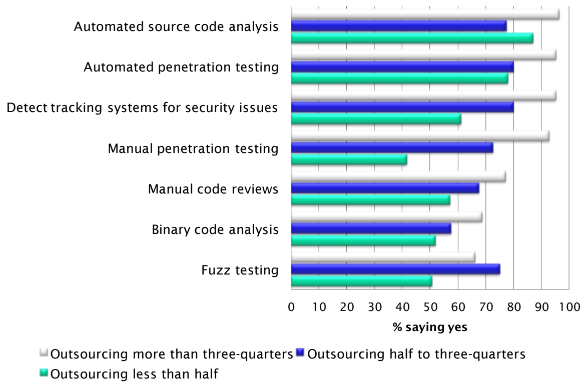
Figure 14: Do you require outsourcers to test applications for the following errors?



In order to ensure that applications are tested thoroughly, including at different stages of the software development lifecycle, organisations should specify the sorts of security testing techniques that must be used by their outsourcers.

As Figure 15 shows, the majority of organisations interviewed take the trouble to specify what testing techniques should be used, with the greatest efforts being taken by those in the "guru" group. However, this also means that the organisation doing the outsourcing must clearly understand the benefit of each of these approaches and what value they bring to the overall testing process in order to be clear about what they require to be used.

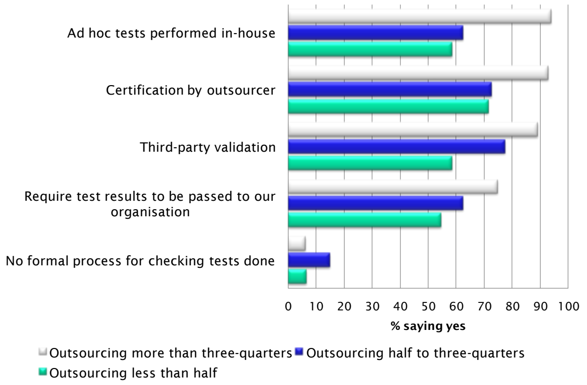
Figure 15: Which methods must outsourcers use for testing applications?



Finally, it is one thing to require that applications are tested for security defects before they are delivered, but how can the organisation that is outsourcing development of an application ensure that those tests have been carried out?

As Figure 16 shows, the vast majority of organisations either perform their own tests or require some form of validation of the testing results. This is positive, although those that have not taken the trouble to define what security tools and procedures should be used in development, as well as how applications should be tested by outsourcers, may find themselves with a delayed project and, potentially, cost overruns as application flaws are uncovered just when organisations thought the application was ready to be put into productive use.

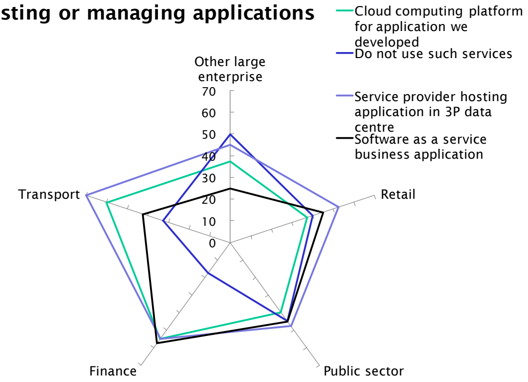
Figure 16: How do you ensure security tests have been carried out?



7. Outsourcing to external service providers

A fast-growing strategy being seen among organisations today is that of the hosting and management of their software applications to external services providers. Figure 17 shows that the use of these services is greatest among those vertical industries that are the most reluctant to outsource the actual development of software applications—namely, financial services and transport organisations.

Figure 17: Use of external service providers for hosting or managing applications

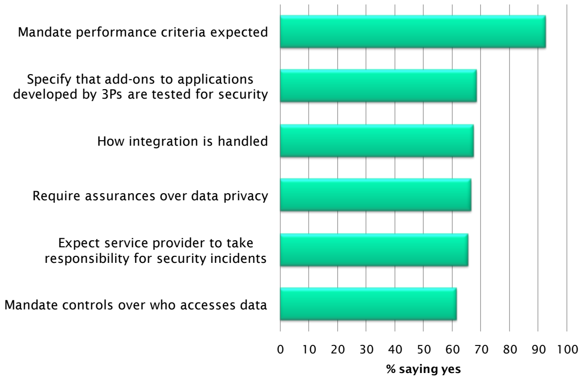


In these vertical industries in particular, organisations are most likely to develop their own applications for hosting and management by outsourced providers, or to use services such as Software as a Service (SaaS). Where organisations use external service providers to host in-house developed code, they will often rely on those partners or other third parties to provide add-on code and other services that extend the value of the software. With SaaS, integration with other internal systems must be achieved, often requiring some level of customisation or add-ons to code that could impede the performance of other applications.

This survey looked to uncover the rigour that is used in gauging the security of the services provided by such outsourced service providers. Figure 18 shows that security is a key criterion for many organisations that are outsourcing their application hosting to external service providers.

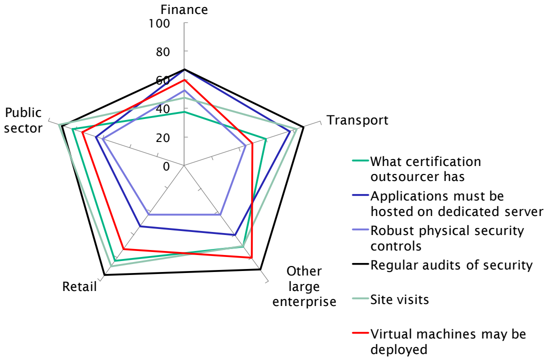
Although the results do not vary much by industry, organisations in the “guru” group are applying the most stringent requirements to outsourcing contracts—namely, those in the public sector and retail organisations—and still slightly outperform those in other industry sectors.

Figure 18: What criteria are used to gauge the security of services offered?



This same pattern can be seen in Figure 19, which shows that those in the “guru” group require the most strict security architectures from their outsourced service providers. However, financial services organisations could do more to learn from their peers in other industries and should consider beefing up their requirements for security.

Figure 19: What security architecture do you require from external service providers?



8. Conclusions

As this report shows, successful outsourcing benefits from an awareness of the likely challenges and risks that outsourcing can pose. For those organisations with the most experience, success is much more likely, and their established best practices can provide a roadmap for others to follow. The stark differences in many places uncovered between this group of leaders, and those with less experience in development outsourcing, demonstrates a major gap between what can be done, and what many are actually doing.

Making use of the best practices detailed in this report, based on the analysis of the responses from the "guru" group, should provide anyone looking at outsourcing development with greater peace of mind. Creating upfront security requirements and deliverables, as well as specifying the means through which they will be measured, will lower risk and result in a more secure work product, delivered on a more predictable schedule, that will also require less maintenance over time.

With the proper safeguards built into outsourcing projects, organisations will be able to achieve their ambitions of increased speed of software application development and reduced costs—at the same time as they shield themselves from the risk of project failure. This will also allow them to build repeatable processes that can more easily be repurposed to ensure the success of subsequent projects undertaken.

These safeguards include not only taking the time upfront to ensure that all expectations and responsibilities are built into a workable contract, but also that all applications have security built in from the ground up and that they are tested for security as a requisite for acceptance.

As well as this, organisations outsourcing application development must ensure that they have the right to audit the application, or have it independently verified, and that remediation processes are in place for dealing with any flaws uncovered.

Dealing with these processes is not only becoming more important as application development outsourcing increases, but also as more organisations undertake newer, fast-emerging types of application outsourcing where applications, including the data they contain, are hosted by third parties, or where service providers write add-ons to applications, such as is increasingly happening with delivery mechanisms such as Software as a Service (SaaS). Best practices gleaned from more traditional outsourcing projects will be of help in deriving greater value and reducing risk in these types of services as well.

Table 4: Summary of best practices for outsourcing of application development
Take time upfront to consider the baseline goals for each project, especially regarding requirements related to staff expertise at outsourcer.
Establish the appropriate level of security that must be built into development procedures for each application and write these into the contract.
Ensure that remediation processes are built into the contract defining actions to be taken should things go wrong.
Define the appropriate application development tools and procedures to be used and stipulate these in the contract, including the right to audit the application.
Specify in the contract what security tools and techniques must be used in order to guard against applications being delivered that contain vulnerabilities.
Make outsourcers responsible for initial testing of applications and specify what outsourcers should test for and what testing methods they should use.
Do not leave all testing up to the outsourcer. Organisations should perform their own tests or require independent validation prior to acceptance.
Extend the same best practices to fast-emerging forms of outsourcing, such as cloud computing or Software as a Service.
However, in such environments, demand greater controls over the physical security of outsourcing providers.

APPENDIX A

Interview sample distribution

The information presented in this report was derived from 200 interviews with those responsible for outsourcing of software application development from those undertaking significant amounts of outsourcing among the largest organisations in five vertical sectors in the UK and the US. The interviews were completed in September 2008.

Distribution of the sample by geography and industry was as follows (Figures 20 and 21):

Figure 20: Sample by geography

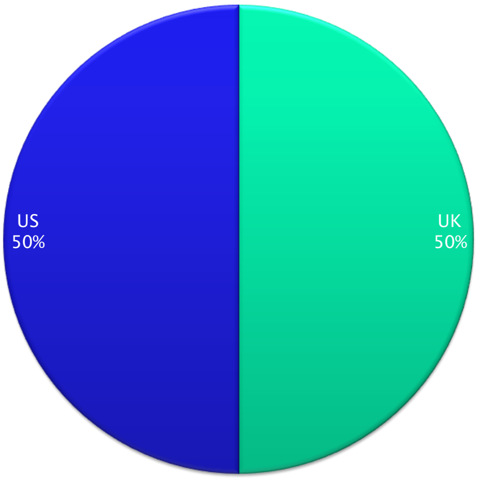
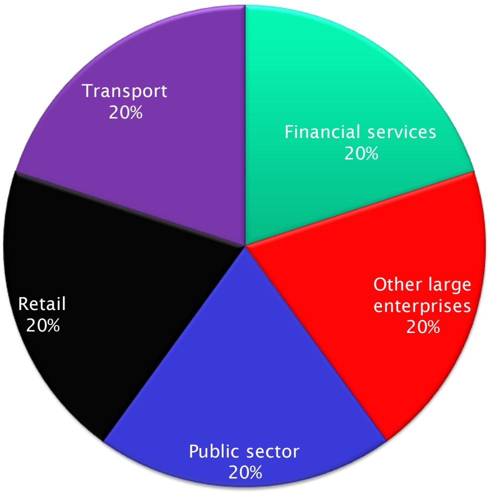


Figure 21: Sample by industry



About Ounce Labs

Ounce Labs' industry-leading enterprise security source code analysis solutions enable organisations to analyse their applications to identify, prioritise and eliminate software security vulnerabilities. Ounce delivers the enterprise-scale features that empower analysis across a wide portfolio of applications, with patented code analysis technology pinpointing confirmed vulnerabilities at the line of code. Only Ounce features the automated workflow and open architecture that enterprises demand, helping organisations such as EDS, IBM, Intel, Lockheed Martin, MFS, the U.S. Government Accountability Office, Unisys and VeriSign, to strengthen application security through their existing development and security processes, and protect confidential information enterprise-wide. Ounce also helps organisations to verify compliance with internal policies and industry mandates including PCI DSS, FISMA, HIPAA and others. For more information, please visit www.ouncelabs.com.

Media Contacts:
Rachel O'Connell
Ounce Labs
781.547.7016
Rachel.OConnell@ouncelabs.com
http://www.ouncelabs.com

Brenda Menard
Davies Murphy Group
781.418.2435
ounce@daviesmurphy.com
http://www.daviesmurphy.com

OUNCE LABS

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with firsthand experience of ITC delivery who continuously research and track the industry in the following key areas:

- Business process evolution and enablement
- Enterprise solutions and integration
- Business intelligence and reporting
- Communications, collaboration and mobility
- Infrastructure and IT systems management
- Systems security and end-point management
- Utility computing and delivery of IT as a service
- Sustainability and environmental issues
- IT delivery channels and practices
- IT investment activity, behaviour and planning
- Public sector technology adoption and issues
- Integrated print management

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption—the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, HP, IBM, T-Mobile, Xerox, Vodafone, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Sponsorship of specific studies by such organisations allows much of Quocirca's research to be placed into the public domain at no cost. Quocirca's reach is great—through a network of media partners, Quocirca publishes its research to a possible audience measured in the millions.

Quocirca's independent culture and the real-world experience of Quocirca's analysts ensure that our research and analysis is always objective, accurate, actionable and challenging.

Quocirca reports are freely available to everyone and may be requested via www.quocirca.com.

Contact:
Quocirca Ltd
Mountbatten House
Fairacres
Windsor
Berkshire
SL4 4LE
United Kingdom
Tel +44 1753 754 838

quocirca