

IT Security – Bridging the Gap Resolving the Paradox of IT Security

Contacts:

Jon Collins
Quocirca Ltd
Tel +44 1285 771433
jon.collins@quocirca.com

Lisa Taylor
Computer Associates
Tel +44 1753 241755
lisa.taylor@ca.com

There is a paradox at the heart of corporate IT security. Despite a clear idea that IT security works best when considered within the strategic context of a corporate security policy, companies are deploying products tactically rather than implementing comprehensive security solutions. IT departments are not engaging sufficiently with the business to fully scope security requirements and understand the business risks to be mitigated by any IT security deployment. Meanwhile, the IT industry should shoulder some of the blame for failing to provide products that are secure out of the box.

- **IT security is a business issue, to be solved holistically and from within**

Companies see business drivers as the best starting point for security solutions, with the top two drivers being business continuity and information protection. In addition, the most important security benefits are also customer facing, in terms of improved trust and providing better services. Despite the emphasis on external threats in the media, companies see the major risks as internal, either from human incompetence or computer system failure. They feel an appropriate combination of built-in security features of technology products and better operational processes would enable these risks to be minimised.

- **Business users are not being involved in security decisions**

Despite this business focus, respondents do not see IT security as an area that business users should get involved in, despite noting that the board should play a greater role in policy definition. This implies a contradiction - respondents agree that security is a business issue, but largely they want to treat it themselves.

- **Tactical security solutions are taking precedence over strategic solutions**

Companies are not managing to implement security in the round. While most companies are working towards the definition and implementation of a corporate security policy, only a minority feel it has been implemented adequately. Similarly, the technologies associated with a holistic approach (such as centralised management) have been implemented by less than half of the companies surveyed. Failures are put down to the ineffectiveness of existing products and solutions, and wasted consultancy.

- **Companies want to define, implement and manage their own security**

Companies don't want to depend on others for security: there is very little interest in handing over responsibility to third parties, either for consultancy, deployment or external service provision. This is largely an issue of trust, driven by reputation and personal experience. The only area that companies would feel comfortable handing over any responsibility is in security audits and reviews. This is an area where companies are particularly weak.

- **Cost is the least important criterion for judging security solutions.**

Companies would prefer a one-off payment (or even monthly subscriptions) to yearly licenses, but more importantly, security solutions need to be compatible with the existing infrastructure. Quality, flexibility, success rate and manageability are secondary. This does not mean that cost is unimportant – rather, it is of concern once the other criteria have been met. Respondents would prefer ongoing security costs to be an intrinsic part of IT maintenance. While this is true in the majority of cases, it could be better.

- **Security needs to be provided in the box, integrated and managed centrally**

Just as companies feel that existing products are not as secure as they could be, so they see that major security improvements should come from IT products themselves in the future. Unfortunately, hardware and systems vendors do not have a good reputation in this area, which confirms the feeling that security has been treated as an add-on rather than a primary concern in the past. Integration is the key enabler, in particular to enable the centralised management and control of security, and to provide a foundation for the safe running of the business.

RESEARCH NOTE:

The information presented in this report is derived from 1209 online interviews completed in June 2004. Respondents were predominantly IT professionals, of all ranks and persuasions, representing a mixture of supplier and end user organisations. The views outlined here are therefore representative of the general IT community.

CONTENTS

1.	INTRODUCTION	3
2.	SECURITY IS ABOUT BUSINESS CONTINUITY	3
3.	APPROACHING IT SECURITY	3
4.	POLICY PROGRESS IS SLOW.....	4
5.	SUITABILITY OF SOLUTIONS	5
6.	SECURING THE FUTURE	6
7.	NOT TRUSTING TO OUTSOURCING	7
8.	DISCUSSION.....	8
	ACKNOWLEDGEMENTS	9
	APPENDIX A – INTERVIEW SAMPLE DISTRIBUTION	10
	ABOUT QUOCIRCA.....	11
	ABOUT COMPUTER ASSOCIATES	12

1. Introduction

This report summarises some of the findings of an online research study conducted in June 2004. The study explores how IT security solutions are being defined and deployed in the corporate environment.

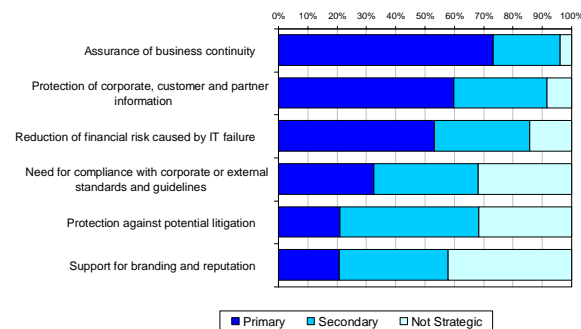
Opinions were gathered from 1209 respondents who completed a Web based electronic survey. Respondents were largely IT managers and professionals, with the remainder including business managers, business professionals, consultants and others. The distribution of respondents by job function, company size and geography is detailed in Appendix A.

The study was designed and analysed by Quocirca Ltd on a completely independent basis.

2. Security is about Business Continuity

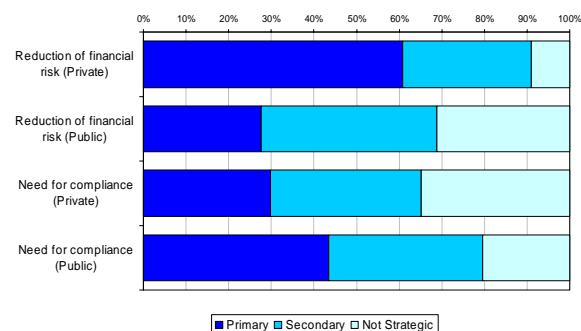
Business failure is not an option, according to the respondents of this survey – nearly three quarters said business continuity was of primary importance to their organisations. This is important, particularly as the majority of respondents were IT focused. Second in the rankings was information protection, followed by protection against financial risk (Figure 1).

Figure 1
What are the strategic business drivers to IT security in your organisation?



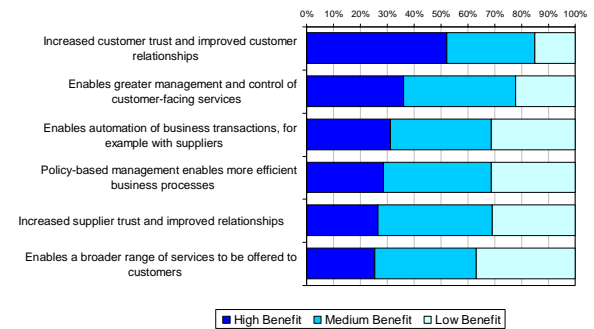
While compliance is garnering much media attention, our research shows that only a third of respondents see it as a primary strategic driver. Where most of the drivers were similar across sectors and geographies, this was not the case for financial risk and compliance between the public and private sectors (Figure 2).

Figure 2
Strategic Drivers (Public and Private Sector)



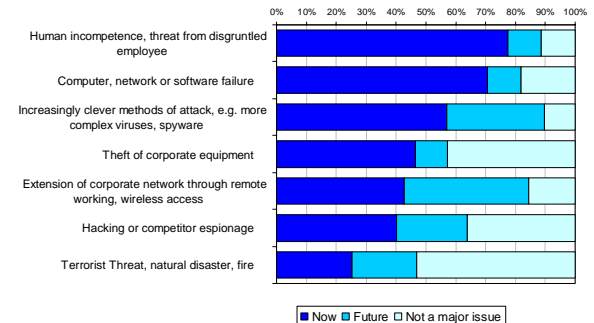
Meanwhile, while legal protection and reputation are seen more as of secondary than primary importance, respondents do see security as a mechanism for improving relationships with customers (Figure 3). More IT-related benefits, including better automation and policy-based management, are seen as less beneficial.

Figure 3
What additional business benefits do you see from IT security?



Given these drivers and benefits of security, it is worth reviewing the causes of security risk. There is no room for hype here: the biggest risks come from inside the organisation, in the most part consisting of human error and technical failure. Perhaps it was ever thus, as Napoleon was reputed to say, "Never ascribe to malice that which can adequately be explained by incompetence," (Figure 4).

Figure 4
What do you feel are the major causes of corporate data risk, now and in the future?



These "internal issues" are currently seen as far greater risks than external attacks, though the latter are expected to grow in impact. Again, there is a question of media attention here. External threats are more newsworthy than internal threats, and while respondents may not be experiencing major issues caused by hacking and virus attacks, they fear that they may one day do so. Remote working and wireless access are also seen more as future threats than current issues.

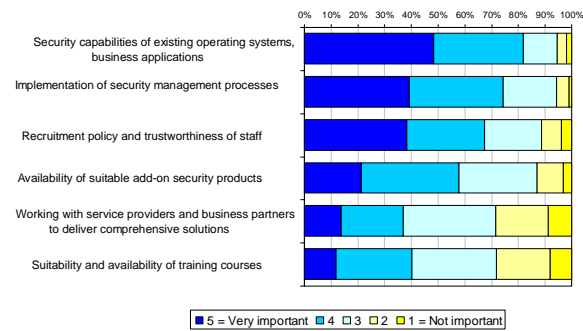
To summarise the findings of this section, the major role of IT security remains to assure business continuity against the joint threats of human error and system failure. There are other reasons, but none should be shaping security policy as much as these fundamental drivers.

3. Approaching IT Security

Given the need for comprehensive IT security, what do companies feel would be the preferred starting point? The vast majority of respondents (over 80%) would like to see security features built into existing operating systems and

applications, compared to under 60% that consider add-on security products to be an enabler (Figure 5).

Figure 5
What do you feel are the most important enablers to the delivery of IT security

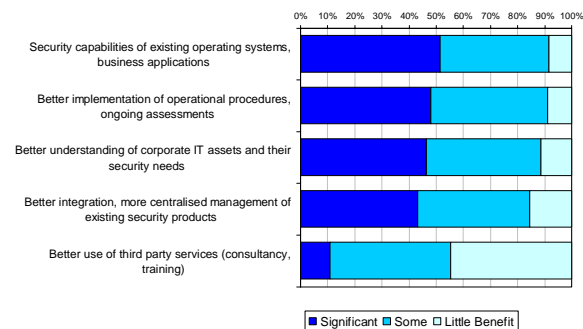


Indeed, the theme that IT vendors are not sufficiently ensuring the security of their own products, repeats throughout this survey.

Interestingly, the second and third enablers in terms of importance are nothing to do with technology, rather they are concerned with processes and people. Perhaps most noticeable about the results, is the fact that companies would prefer to resolve issues themselves rather than relying on third party advice, services or even training. This could be for a host of reasons, from the real inadequacy of the services sector to pure psychological resistance, but it is clear that security providers have a challenge on their hands.

These findings are further confirmed in Figure 6, where once again, third parties come in last. Indeed, as we shall see in Figure 9 later, the only area that respondents see an increased role for external suppliers is in compliance assessment. Section 7 covers the role of such suppliers in more detail.

Figure 6
In which ways do you think you could benefit from "working smarter" to approach IT security?

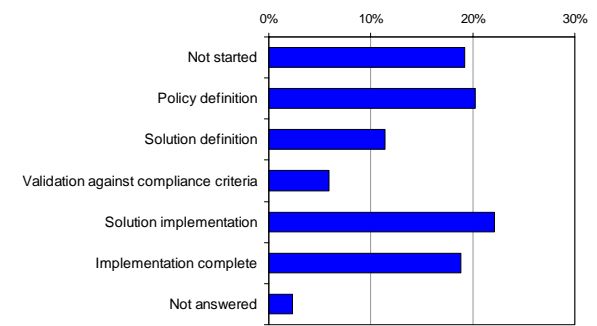


So, given that companies are so keen to do it for themselves, how exactly are they getting on?

4. Policy Progress Is Slow

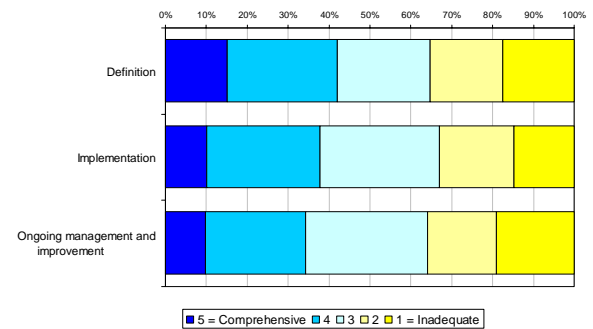
It is clear from the findings thus far, that companies have a reasonable grasp of what they want from IT security, and they also know what would be a good starting point for security solutions. So, how are they getting on in practice? In the perfect world, a company would work through a number of stages (Figure 7) to define and implement appropriate security solutions. While the results give some cause for optimism, there is clearly much more progress to be made.

Figure 7
What stage has your organisation reached, relative to implementing a comprehensive security policy?



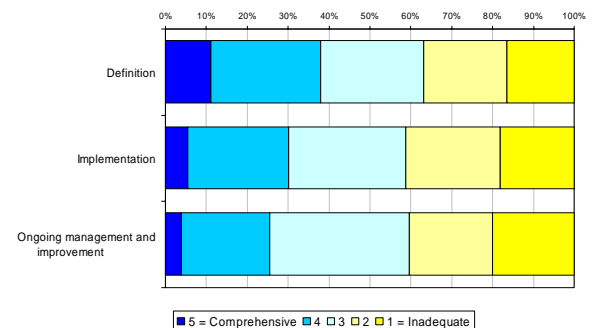
The good news is that only 19% of respondents have not started to define or implement a security policy, and 59% already have a security policy defined. Meanwhile, the bad news is that only 18% of companies have completed such an implementation. There is a broad range of opinion as to how well the job has been done, with 42% of respondents feeling that their security policy is adequate, and a lesser number feeling they have a comprehensive security implementation (Figure 8). This is unsurprising if companies are still working through the process.

Figure 8
Do you feel your corporate security policy has been defined and implemented adequately inside your organisation?



Implementation figures are less good if we take the public sector by itself (Figure 9).

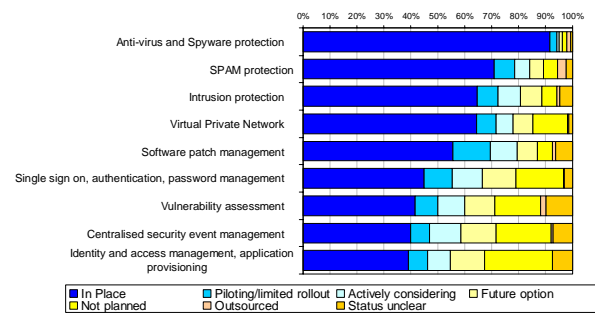
Figure 9
PUBLIC SECTOR: Do you feel your corporate security policy has been defined and implemented adequately inside your organisation?



Despite this lack of strategic completeness, there is no shortage of specific products being implemented. Most companies feel they have all the antivirus protection they need, and the current focus is on Spam, Firewalls and VPN,

with patch management attracting the most pilots (Figure 10).

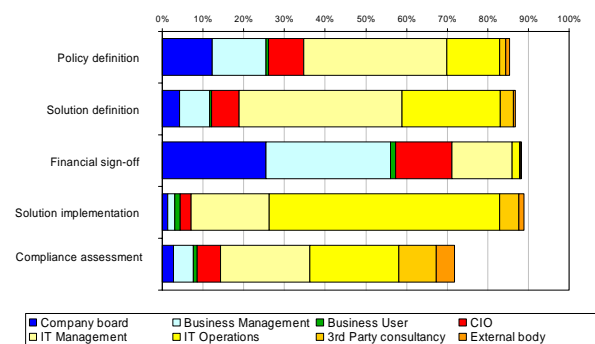
Figure 10
Which of the following applies to the deployment and use of these security applications?



Though centralised security event management is seen as a major requirement, only 40% of respondents have implemented such a facility – clearly tactical solutions are winning out. Centralised management is a key requirement for the future, as discussed in section 6 below.

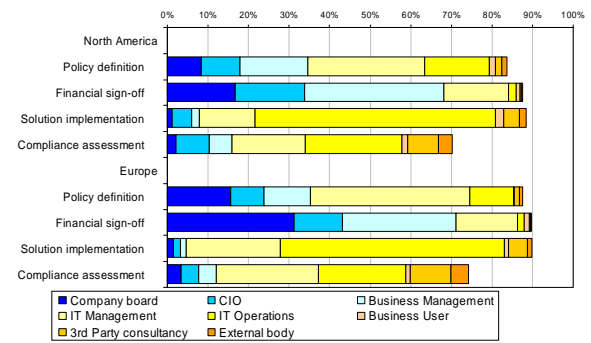
One of the most important areas of security policy is allocation of responsibility. When we asked who was responsible for security, we received the following answers (Figure 11).

Figure 11
Who is responsible for security in your organisation, in the following areas?



There are some striking differences between Europe and North America when it comes to responsibilities. In Europe, the company board is roughly twice as involved in the activities of policy definition, financial sign-off and compliance assessment. Meanwhile, North American CIOs have a greater role in these activities and in solution implementation than their European counterparts (Figure 12).

Figure 12
Who is responsible for security in your organisation (North America and Europe)



While the board and business management already have a role to play in financial sign off of security solutions, respondents agreed they should have a greater role in the definition of the policy. This is shown by comparing two sets of results – who is currently responsible, and who should be responsible, for the security policy (Figure 13). It is not the case for business users however, who are considered as having little to add to the policy debate. Common sense suggests that this is a failing – does the IT department really know how the business runs better than the business users?

Figure 13
Who is responsible for security policy and compliance in your organisation, and who should be?

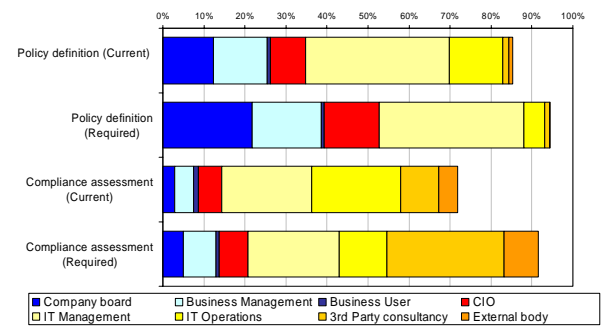
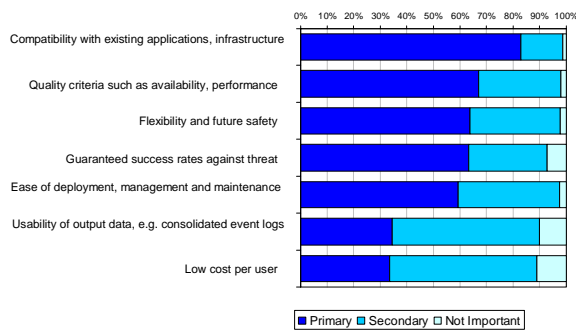


Figure 13 also shows a role for third parties in compliance assessments. Indeed, companies would be prepared to make more extensive use of third parties in this role, than they do currently.

5. Suitability of Solutions

The results so far indicate that companies do want to deliver comprehensive IT security solutions. This is illustrated further in Figure 14, where 83% of respondents believe the most important criterion is compatibility with what is already there. This is even more important than guaranteed success against threats, which is only fourth on the list behind availability, performance and future safety.

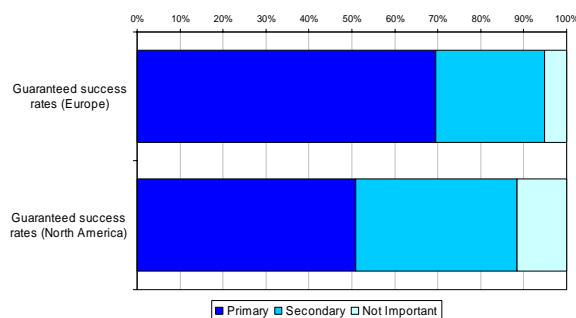
Figure 14
What would be your criteria for judging the suitability of a security solution?



Cost is right at the other end of the scale, below every other criterion, even usability of the output data. This is not to say that cost is not important. Nearly 90% of respondents agree that cost is at least of secondary importance, just like all the other criteria. It is just that the other criteria take precedence: once they are fulfilled, then cost plays a part.

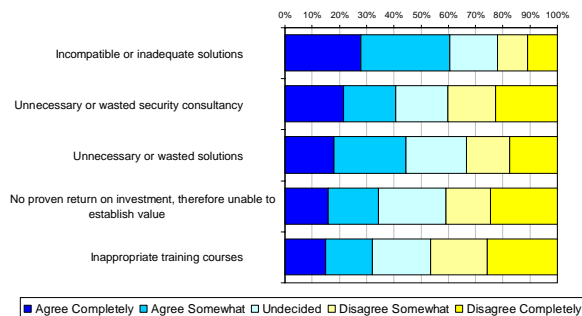
Incidentally, the only significant difference between Europe and North America is the importance of a guaranteed success rate (Figure 15).

Figure 15
What would be your criteria for judging the suitability of a security solution (Europe and North America)?



Perhaps the emphasis on compatibility is understandable when we consider some historical reality – the reasons for wasted budget in the past can be put down to incompatible or inadequate solutions, not to mention resources wasted on security consultancy (Figure 16).

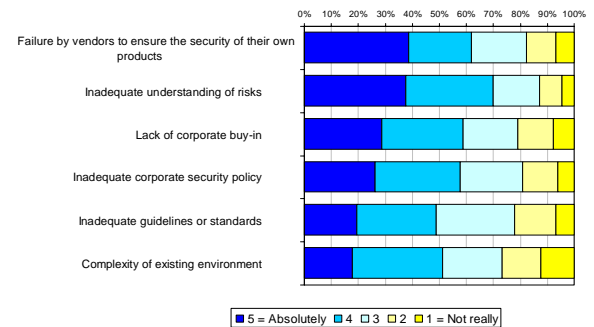
Figure 16
How do you feel security budget resources have been wasted in the past?



So, what has gone wrong? In the definition phases, the top two reasons are the lack of existing product security and the

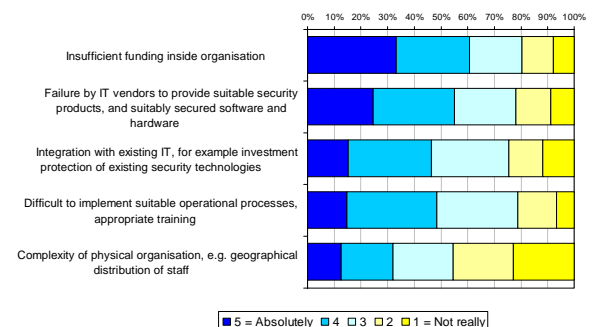
failure to understand business risk, though corporate issues also play a part (Figure 17). The inadequate understanding of risk could be seen as the top reason, with 70% of respondents ranking it as a "4" or above. This is quite telling – once again it shows that IT security starts and ends with the business.

Figure 17
What reasons would you give for the failure to define effective security solutions?



The lack of corporate buy-in is also telling – if the business was sufficiently engaged it would also be prepared to fund what it wanted, but as things exist this is not the case as shown in Figure 11 previously. This also links to the main reason for the failure to implement adequate security solutions, namely insufficient funding (Figure 18).

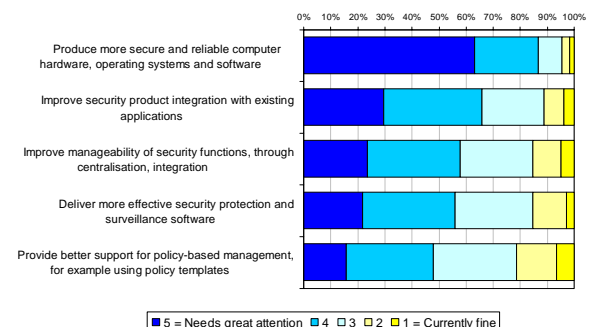
Figure 18
What reasons would you give for the failure to implement effective security solutions?



6. Securing the Future

As for the future, what should be done by the IT industry? First and foremost, it should be producing more secure and reliable systems and software (Figure 19).

Figure 19
What do you think needs to be done by the IT industry in the future to guard against security problems?



Better reliability, with improved integration and manageability, support the trend towards better packaging of security solutions geared around the needs of applications. At the moment this is mainly aimed at email security, corresponding to the findings in Figure 10. However, security solution bundles are likely to support a broader range of applications in the future.

For the companies involved in the survey, the major step to be taken concerns how security measures are managed: integration into a centralised management facility is the biggest requirement for the future (Figures 20, 21). There is also less desire for individual management of point solutions, and once again, there is little interest in external management, either by consultants or service providers, now or in the future.

Figure 20
How are the majority of current security measures managed?

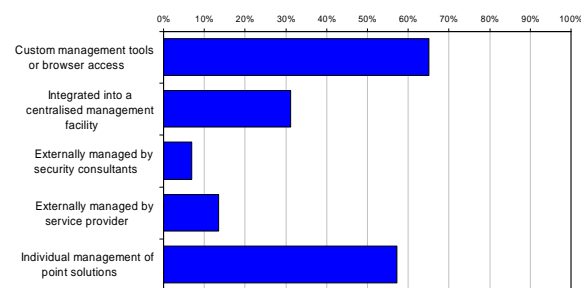
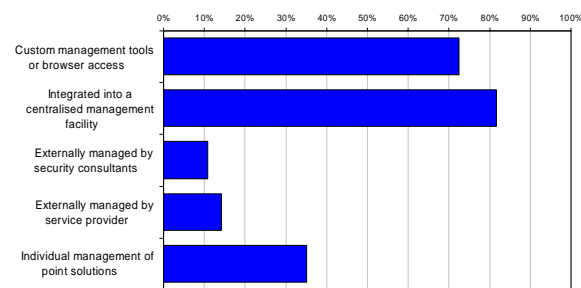


Figure 21
How SHOULD security measures be managed?



Note there is a discrepancy between Figure 20 and Figure 10 concerning centralised management. Figure 10 says that 40% of respondents have implemented centralised event management, whereas in Figure 20, only 32% of respondents say that security products are managed using a centralised facility. This may be explained by the fact that "centralised management" is a broader concept than "centralised event management". In either case, the leap to 82% wanting centralised management in Figure 21 speaks for itself.

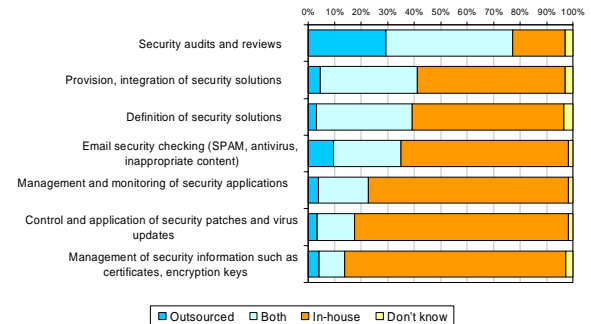
7. Not Trusting to Outsourcing

One of the themes of this report has been how companies do not want to trust their security to third parties (service providers, consultants and integrators). Is there any cause for optimism for these organisations?

At first glance, the only real opportunity for outsourced consultancy is seen as security audits and security reviews.

About 10% of respondents also considered there be to be a place for service provision of e-mail security checking. However, any hands on security activities are seen as the domain of the organisation (Figure 22).

Figure 22
What security roles do you think external consultants and service providers should take, and what should be kept in-house?

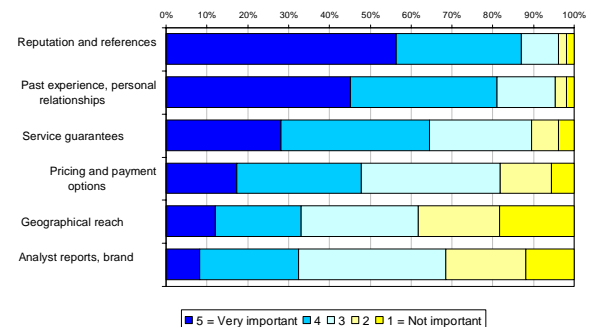


It's not all such bad news for the consultancies however, if we look at where companies would be prepared to share some of the responsibility. Here, about a third of the respondents agreed that there was a place for external providers to get involved in the definition and deployment of security solutions. There was less of a place for security checking of e-mail, and even less for management and monitoring of security applications. Where companies wanted the most control was in the management of their own security information and environments. Companies do not want to relinquish *any control* over their own security.

The desire to keep control does not close the door to providing security as an externalised service. It does emphasise the need for self-service, that is to ensure that management, configuration and reporting facilities are accessible in-house, wherever the service is being provided.

As mentioned before, the fact that companies don't feel able to depend on external suppliers might be for a number of reasons, some of them real and some of them perceived. We can gain some understanding of why this might be, by looking at the criteria that companies use to select security companies (Figure 23). The top two reasons are to do with personal knowledge and perception. No 1 is reputation and references, followed by experience and personal relationships. In other words, use of external providers is largely down to personal trust.

Figure 23
What criteria would you use to select external consultants and security service providers?



Service providers' own capabilities (guarantees, payment options) form the second set of rankings, and last of all is the

more third party information such as brand recognition, or information from analyst reports. There is no substitute for experience.

Security audits and reviews are the one area that external companies have a genuine foothold. Ironically, while the majority of respondents see audits as necessary on a planned basis, this bears little resemblance to how often such audits take place. Over a third of respondents say they have never had a security audit, and only around 25% say that audits have taken place with any regularity (Figures 24, 25). Perhaps audits are the best way for third parties to start to develop a trust relationship with end-user companies. While this is the one area that companies are able to grasp, it would appear to be the one thing they are unable to do for themselves.

Figure 24
How often do you think third party security audits of your IT infrastructure are necessary?

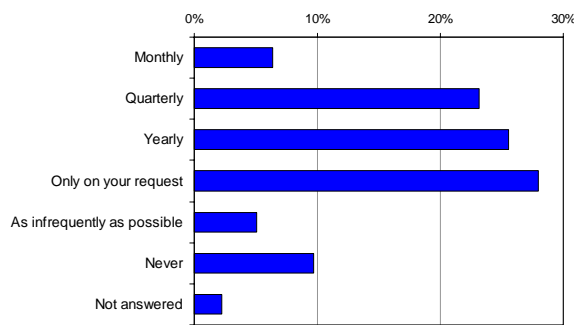
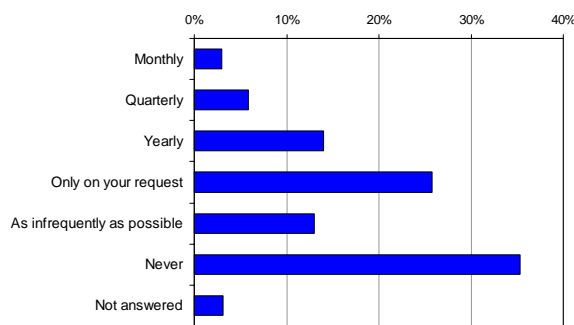


Figure 25
How often do they actually take place?



Where there is some room for manoeuvre is how security is paid for. Currently the main modes of payment are fixed payments and yearly upgrades. More flexible payment models make up only a small portion of security payments. However companies would be prepared to make more use of flexible payment models, either integrated as part of an external service or on a monthly, subscription basis (Figures 26, 27).

Figure 26
How are you currently paying for security solutions?

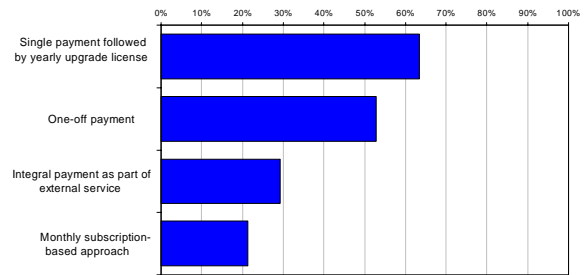
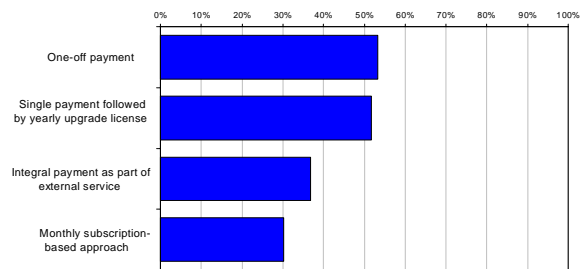


Figure 27
How would you PREFER to pay for security solutions?



8. Discussion

Security is a big issue at the moment, and rightly so. Viruses have cost the global economy billions, so we are told, and SPAM is the modern malaise, with unwanted messages feeding on electronic communications paths like plague rats. While media attention is largely focused on what damage outsiders might cause to companies however, let us not be distracted from the reality, that the biggest security risks are on the inside. Companies know this, and IT departments know this, but all the same more attention is spent on mitigating outside threats, which are as media-driven as they are media-reported.

The result is that companies feel obliged to implement the solutions that the media say are the most vital. There is nothing wrong with deploying firewalls or VPN software (as long as they do the job), but tactical deployments are distracting companies from the real challenge, of defining and deploying a corporate security policy that takes a holistic view of the business risks and enables the implementation of a comprehensive solution.

Interestingly, one of the main reasons for failing security is incomplete understanding of risks, as well as lack of funding. This ties with the desire to have the business more involved in the definition of security policy, but it contradicts the fact that IT wants to be 100 percent in charge of implementing security solutions. Clearly there has to be a balance between business and IT, but equally, this balance has not yet been struck, and a holistic view of risks is not being taken. Most tellingly from this research is the number of companies that have never had a security audit. Perhaps this means the companies already know exactly what their security situation is, but we doubt it.

Speaking of audits, please spare a thought for the external companies that want to provide security services. These are largely given short shrift by the companies they are trying to serve. There is probably a greater place for external providers but they are going to have to earn their stripes, perhaps starting with audits, and building up a trust relationship.

Acknowledgements

This kind of research is crucial to all of us in the business and ITC community - suppliers and customer organisations alike. We would therefore like to thank all of those participants who contributed so generously towards a better understanding of issues in this important area.

Appendix A – Interview Sample Distribution

The primary research data presented in this report is from 1209 responses to a Web based questionnaire gathered in June 2004. The following charts illustrate the distribution of this sample in terms of industry (Figure 28), company size/type (Figure 29), respondent role (Figure 30) and geography (Figure 31).

Figure 28
Respondents by Industry

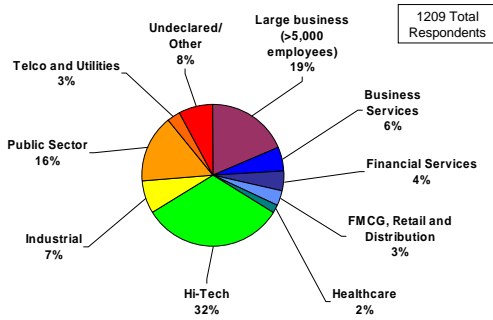


Figure 29
Respondents by Size/Type of Company

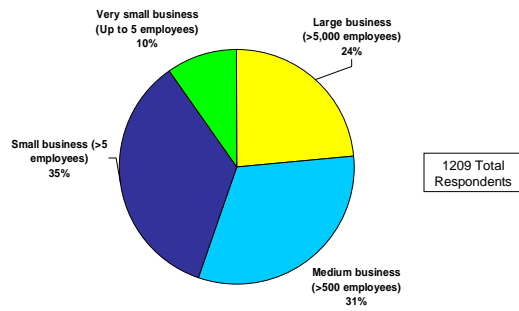


Figure 30
Respondents by Role/Viewpoint

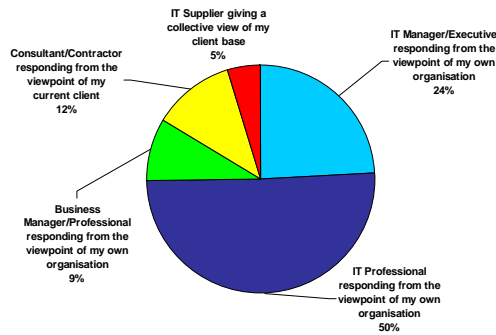
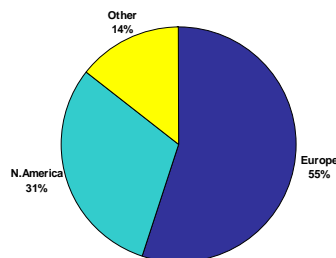


Figure 31
Respondents by Geography



About Quocirca

Quocirca is a research and analysis company with a focus on the European market for information technology and communications (ITC). Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry in the following key areas:

- Business Process Evolution and Enablement
- Enterprise Applications and Integration
- Communications, Collaboration and Mobility
- Infrastructure and IT Systems Management
- Utility Computing and Delivery of IT as a Service
- IT Delivery Channels and Practices
- IT Investment Activity, Behaviour and Planning

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 its customers improve their success rate.

Quocirca has a pro-active primary research programme, regularly polling users, purchasers and resellers of ITC products and services on the issues of the day. 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 Morgan Stanley, Oracle, Microsoft, IBM, CA and Cisco. Sponsorship of specific studies by such organisations allows much of Quocirca's research to be placed into the public domain. Quocirca's independent culture and the real-world experience of Quocirca's analysts, however, ensures that our research and analysis is always objective, accurate, actionable and challenging.

Most Quocirca research reports are available free of charge and you can receive these automatically upon publication, by registering at http://www.quocirca.com/report_signup.htm. Copies of past reports from Quocirca's research library may be requested via www.quocirca.com.

Contact:

Quocirca Ltd
Mountbatten House
Fairacres
Windsor
Berkshire
SL4 4LE
United Kingdom

Tel +44 1753 754 838
Email info@quocirca.com



About Computer Associates

Founded in 1976, Computer Associates International, Inc. (CA), the world's largest management software company, delivers software and services across operations, security, storage, life cycle and service management to optimise the performance, reliability and efficiency of enterprise IT environments.

CA is the recognised leader in management software with unparalleled depth and breadth in security management. Its security management solutions enable organisations to consistently enforce their security policies, assess vulnerabilities, and monitor and evaluate information to properly protect their assets while enabling business growth.

The eTrust portfolio consists of solutions which enable an extensive view of security comprised of Identity and Access Management, Threat Management, and Security Information Management.

eTrust solutions simplify security management by providing an innovative, comprehensive approach to security. eTrust protects information assets and resources, provides appropriate access to employees, customers and partners, centrally manages security-related administration and coordinates emergency command and control to enable a higher return on investments and compliance with regulatory requirements.

The solutions are open and integrated, and can work with existing security technologies and with an organisation's existing security infrastructure.

CA has maintained its position of technological and business leadership for over 27 years. The Company has obtained more than 200 patents worldwide and has more than 900 patent applications pending. CA is also the first and only global enterprise software company to meet the exacting standards of global ISO 9001:2000 certification. CA continues to evolve its core technologies and best practices to meet the next generation of business challenges and help drive growth.

CA is headquartered in Islandia, N.Y., and operates in more than 100 countries. For more information, please visit <http://ca.com>.

Contact: Lisa Taylor, UK Public Relations
Tel: +44 (0)1753 241755
Email: lisa.taylor@ca.com

