Quocirca Insight Report May 2005

Security Barometer Survey

The Psychology of Security

Contacts:

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

Clive Longbottom
Quocirca Ltd
Tel +44 1189 483360
clive.longbottom@quocirca.com

IT security is high on the agenda of most companies, and so it should be. There are a number of discrepancies however, largely driven by psychological factors. Of particular significance is that existing security policies are seemingly doing little to improve the security of organisations. They should not be seen as an end in themselves, and may be in need of urgent review.

- **Security understanding is still victim to the fear factor**

  In this post downturn age of IT, we would hope that security understanding replicates the increased drive we see towards IT efficiency and effectiveness. However, there is considerable evidence that psychological factors are still as important as they ever were. For example, companies that suffered a security attack in the recent past are significantly more aware that they might suffer a similar attack in the future. Meanwhile, newer threats such as Spyware are – incorrectly – not yet seen as high risk.

- **Policy-based security enhances awareness**

  It should be expected that companies that take a policy-based, proactive stance on security issues, such as companies who have implemented a formal security policy, would be better protected against security threats. The research seems to show that having a full policy and having no policy makes little difference – however, the analysis shows that this is down to lack of awareness of possible threats from those with no policy in place.

- **Security threats are being hyped above those of unscheduled downtime**

  Roughly three times as many respondents had experienced unscheduled downtime due to software or hardware failure, compared to downtime due to security issues. We should not downplay the issues caused by security, indeed, some system failures may be caused by security problems without it being that obvious. However, companies should be treating downtime in the round.

- **Security issues are directly impacting individual productivity**

  Respondents were quick to point out that there would be significant or some impact of security issues on either their individual productivity or as a cost to the business. Indeed, over half of respondents considered that they wasted a day or so every month dealing with security issues. This equates to a significant financial cost to industry. A proportion of respondents (at least 10%) have suffered the impact of some kind of security attack in the past three months.

RESEARCH NOTE:

This report is derived from a study of 3,097 online respondents, conducted in collaboration with The Register Web site, in March 2005. The survey was intended to gauge the relative levels of the most common security threats today. Questions covered the relative threats of IT security issues such as malicious software, spyware and intrusion, in a corporate environment.

Discussion

It was unexpected in the extreme that the presence of a formal security policy in an organisation would seemingly have such little impact on security issues. Even taking into account the "blissful ignorance" of those with no policy leading to the issues being under-played for this group, we would have expected a much more visible difference in results. This inconclusive return from investment in formal policies may be due to a number of factors:

- The policy is centred purely on IT, without looking at corporate security in the round.
- The policy does not cover all of the relevant IT security threats.
- The policy has been inadequately implemented.
- The policy is not being kept up to date.

A piece of advice that this report cannot make too strongly is that companies with existing security policies should review them frequently to ensure they are actually achieving their objectives.

An independent study by the primary research division of Quocirca Ltd.

www.quocirca.com

The Perceived Threat

The initial set of questions determined the perceived impact of security threats, from both a productivity and a cost perspective. Figure 1 shows the potential productivity impact of the different kinds of security attack. While all the threats were seen to have some kind of productivity impact, intrusion, denial of service, malware and fraud were seen as the most significant. Spyware was not seen as posing a significant threat.

Figure 1

Copyright 2004 Quocirca Ltd

How would you rank the potential impact to your organisation's productivity from the following threats?

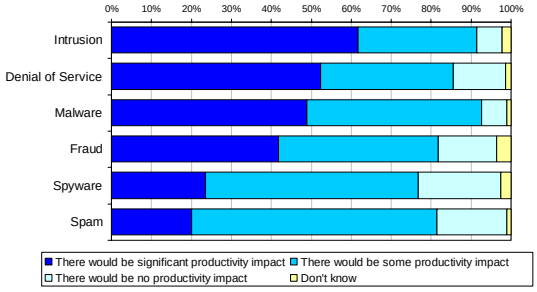
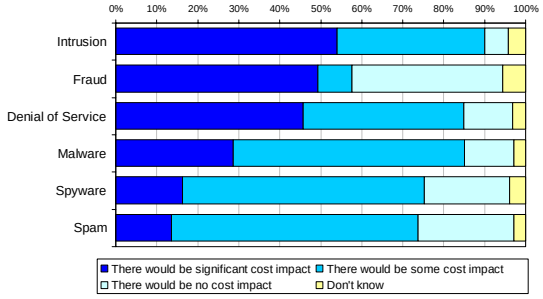


Figure 2 shows the cost impact. The order is similar to that with productivity, but fraud is seen as more significant.

Figure 2

Copyright 2004 Quocirca Ltd

How would you rank the potential cost impact to your organisation?



These findings are important as they give an indication of how organisations perceive the relative risk of security issues, and therefore the relative priority for mitigating those risks. Incidentally, there was no real difference for the responses by role; for example IT management respondents gave much the same answers as non-IT users.

The psychological factor became very clear when respondents were asked about their expectations of security issues happening in the future (Figure 3). In every case (including malware shown here), companies who have already experienced an issue seem to take the threat more seriously (Figure 4).

Figure 3

Copyright 2004 Quocirca Ltd

How would you rank the likelihood of the following occurring in the future?

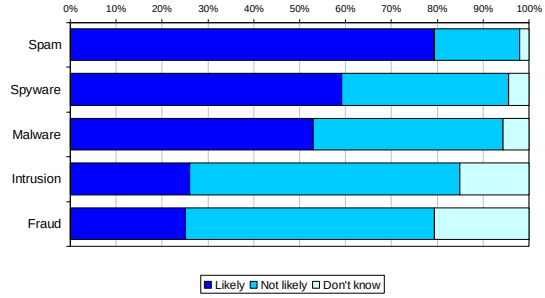
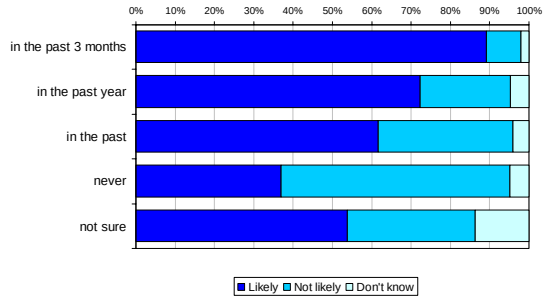


Figure 4

Copyright 2004 Quocirca Ltd

If you have experienced such a threat in the past, how would you rank the likelihood of Malware in the future?



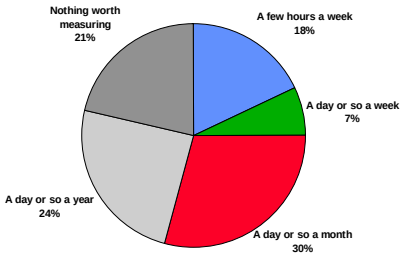
1. The Reality

Having covered the theoretical threat, respondents were asked how they were directly impacted by security issues. Over half – 55% – felt they wasted at least a day per month (about 1 day in 20) due to security problems. This is a significant finding (Figure 5).

Figure 5

Copyright 2004 Quocirca Ltd

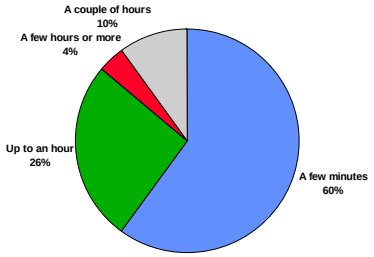
How much time would you consider you waste due to security problems?



As an aside, we asked about Spam: while only 14% of respondents wasted more than an hour on Spam per week, clearly it remains an issue (Figure 6).

Figure 6 Copyright 2004 Quocirca Ltd

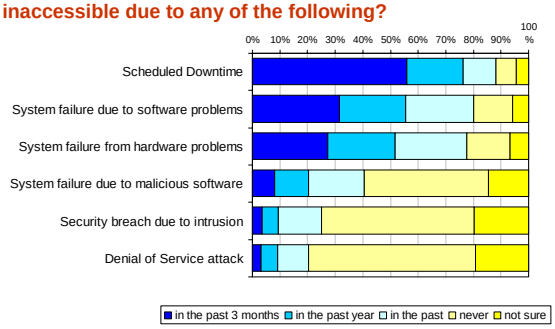
How much time do you personally spend per week dealing with Spam?



While security is clearly important, it is equally important to understand how security issues sit relative to other causes of downtime (Figure 7).

Figure 7 Copyright 2004 Quocirca Ltd

Have your computer systems or web sites been rendered inaccessible due to any of the following?



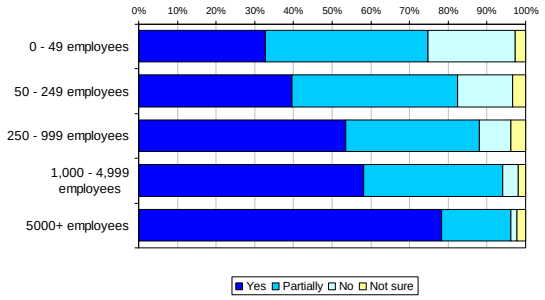
Scheduled downtime is, by its nature, less obtrusive than unplanned failures. Keeping this in mind, failures due to hardware or software problems appear roughly three times more often than security-related failures. There is the potential that such problems are security-related, but we can draw from this that overall system failure, no matter through what cause, needs to be considered in the round.

2. Policy Drivers

Unsurprisingly, larger companies are more likely to have implemented security policies than smaller ones (Figure 8).

Figure 8 Copyright 2004 Quocirca Ltd

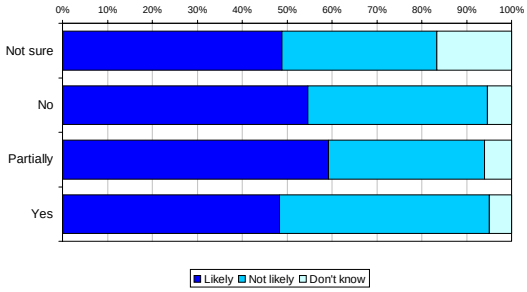
Has your organisation implemented a formal security policy or process?



Less good news is that security policies do not appear to be having any significant effect against the likelihood of threat (Figure 9).

Figure 9 Copyright 2004 Quocirca Ltd

How would you rank the likelihood of a Malware attack occurring in the future?



This could be put down to increased awareness of the theoretical threat or possibly the higher occurrence of formal policies in larger organisations who perceive they are more of a target. We should therefore also look at the impact of policy on the consequential effects of security issues Figures 10, 11).

Figure 10 Copyright 2004 Quocirca Ltd

Have your computer systems or web sites been rendered inaccessible due to malicious software?

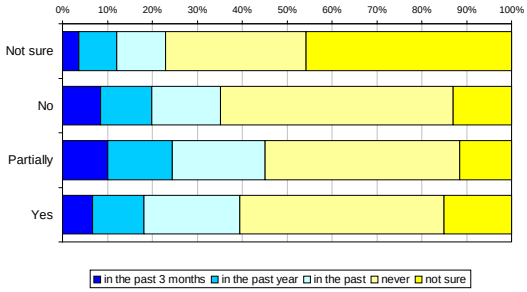
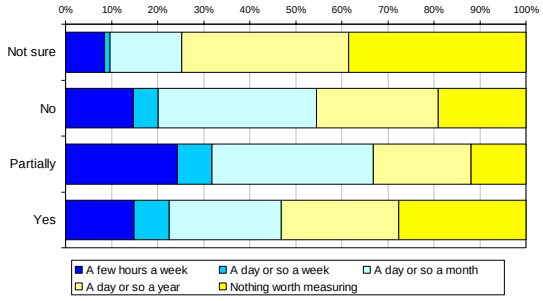


Figure 11 Copyright 2005 Quocirca Ltd

How much time would you consider you waste due to security problems?



At first glance, it would seem that having a security policy in place is no better than not having one, as the differences between these groups are low. Implementing and enacting a security policy is expensive – if there appears to be no difference between the two groups, is it worth it?

What we see here is a typical adoption curve. Those who have no policy in place see fewer problems – they are unaware when a passive or benign virus is present, they do not perceive the denial of service attack as being anything other than that the internet is running slowly. Those with fully implemented policies see more – and react more, even to threats which are not likely to be of high importance. Those with partially implemented policies are in the worst situation psychologically – they can see a lot more than they could before they started implementing a policy, but have only a partial means of dealing with the threat. This is also seen when we look at figure 9 – those with a partial policy feel the most threatened – there is a heightened perception of threat, and a knowledge that not all threats can be dealt with.

Quocirca believes security policies remain important – but must be seen within the overall context of the business. Protection of "Intellectual Property Assets" is not purely a technical issue – we also have the human assets that come and go from our environment at will, as well as security holes such as telephones, fax machines and even the disposal mechanisms for paper mail and other documents. We need to ensure that we include these assets and holes within the overall security policy – and we need to measure against the policies and implement and enact procedures to mitigate against any problem that we do find.

This takes us right to the roots of why security policy should exist. Having a security policy does not stop security issues from happening. A poorly defined security policy is very dangerous – it leads to a perception of security, rather than a reality. However, being aware of the issues – and implementing the capability to deal with them – provides a far more powerful weapon than hiding our heads in the sand.

Appendix A – Interview Sample Distribution

The primary research data presented in this report is from 3,097 responses, derived from an online survey executed in March 2005 in association with The Register Web site. The questionnaire used in this study was designed by Quocirca Ltd. The Quocirca primary research team also analysed and interpreted the results and all work was conducted on a completely independent basis. The respondents were broken down by company size as shown. While the majority of respondents occupied technical roles, 14% occupied non-technical roles (Figure 28).

Figure 12 Copyright 2005 Quocirca Ltd

How large is the organisation you work for?

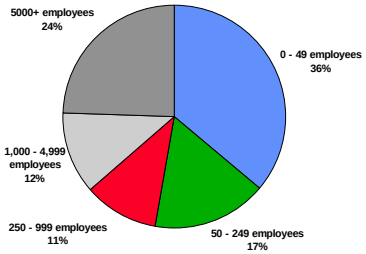
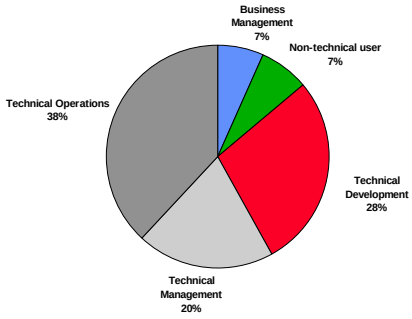


Figure 13 Copyright 2005 Quocirca Ltd

Which of the following best describes your role in the organisation?



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.

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. 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 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, 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. You can receive these automatically upon publication, by registering at http://www.quocirca.com/report_signup.htm. Copies of past reports may be requested via www.quocirca.com.

quocirca

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

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