

## ComputerWeekly – See the Bigger Picture on Data Security

By Clive Longbottom, Service Director, Quocirca Ltd

Excuse me if I rant for a while. This time, it's about security, and how many suppliers are still happy to sell you stuff that you don't need, and to give you part solutions that they pretend are all-inclusive.

OK, there's the legal part of security. We all need to secure our systems, because if we cannot demonstrate that we secure personal information, the Data Protection Act cuts in and it costs us a lot of money.

Is there really any other reason that forces us to go for security? I don't believe so.

Yes, there is the possible impact on your brand of being seen to be insecure. There is the possible financial hit of intellectual property being made available to competitors. There is the possible loss of patent rights through previous disclosure.

There is the time that may be lost in fighting the effects of viruses. But all of these are risks – and it is up to the organisation, not IT security suppliers, how much risk it wants to take.

Surely the main part for a security supplier to play is for it to enable the user organisation to assess its own risk and to create an acceptable risk profile.

The supplier can then help the company make informed decisions on what it is willing to carry as risk and what it needs to spend on to minimise that risk which it is unwilling to carry.

A significant minority of the channel and many systems integrators already take a more holistic view of security. Even a few IT suppliers are doing parts of this, either by being savvy or by partnering with companies that cover physical security. However, most IT security providers tend to become a little economical with the truth when we take security fully in the round.

How many try to baffle you with details of how prevalent the latest virus or denial of service attack is, with no details of what the impact on your business would actually be?

How many times have you been told by an IT supplier that if your electronic documents are not secure, you will be out of business within a week/month/year?

How many have tried to sell you document management tools with the promise that they will be the silver bullet to information security? And how many of these systems allow users to simply print out a document and walk away with it?

Here lies the problem: certain companies that sell IT security are only interested in technology security. The physical world doesn't exist for them – that is someone else's problem.

How many technical security suppliers that have come to see you have pointed out the problems of having fax machines easily available to people as a means of getting information out of an organisation?

How many talk to you about the vetting of personnel, of the need for policies that cover the use of telephones, of the security risk of allowing employees to have briefcases and handbags? How many comment on the positioning of CCTV systems and physical entry into and around your premises?

The assumption is that the presence or lack of policies to cover all these physical security risks is a demonstration of your capability to balance risk against probability of an action occurring.

But you are not allowed to have this luxury in the technical world – the received wisdom is that if you have a computer you must have it completely, technically, secured.

This arrogance of nannying you in the technical world while paying no attention to other areas of your environment breeds complacency – if you have spent millions of pounds on technical security, then surely you are OK?

That someone walks in and takes a ream of paper off the office printer is not seen as an associated security risk.

You can have the best technical security in the world and yet find that all your intellectual property is available on the web due to bad physical security. You can spend all of your revenues on creating completely secure systems and you still won't have security.

Ensure that you talk to companies that look at security in the round and will help you to identify your real security needs based around your own acceptable risk profile. Any IT security supplier that cannot do this should be physically locked out – they won't have a "solution" for this.

### **About Quocirca**

Quocirca is one of Europe's leading independent industry analyst firms. One of its biggest assets is the core team of highly experienced analysts drawn from both the corporate and the vendor communities. This team prides itself on maintaining a bigger picture view of what's going on in the IT and communications marketplaces. This allows all of Quocirca's activities to be carried out in the context of the real world and avoids distractions with fads, fashions and the nuts and bolts of specific technologies. Quocirca's focus has always been the point of intersection at which IT meets "the business".

### **Quocirca Services**

The insight and experience that comes from working as an industry analyst as well as a practitioner allows the Quocirca team to contribute significantly to IT Vendors, Service Providers and Corporate clients. To this end, it provides a range of consulting and advisory services. Details of these, along with some of Quocirca's latest analysis, may be obtained by visiting <http://www.quocirca.com>

Quocirca's primary research involves the surveying of many thousands of technical and business end users each quarter, analyzing their perceptions of the possible impact of emerging, evolving and maturing technologies on their businesses.