

Can you remove the fear-factor from information security?

While virus protection may grab the headlines, the wider issues of reliability and business continuity are what put information security at the top of any senior manager's agenda. But how can mid-sized businesses deal with this increasingly complex security landscape?

Business managers are bombarded daily with fear-inducing stories about trojans and hackers, giving the impression that this is the sum of information security. However the anti-virus and intrusion protection technologies deployed to keep virus and hackers out of a company's systems are only two aspects of a much bigger security picture.

Just as worrying are headlines about accidental loss of data: CDs lost in the post and laptops left on trains. These reveal an important truth about information security: it is as much about managing people as it is about technology and the management issues need to be settled before any technological fixes will work as they are designed to.

Reliability and continuity

They also point to the fact that security is about more than blocking viruses and hackers, and encompasses less publicised issues, such as reliability of information systems and business continuity. In fact, to concentrate on anti-virus or

intrusion protection to the exclusion of this bigger picture is to increase risk to the business not decrease it.

All businesses are reliant on IT and communications. A mid-sized business like yours may not have the vast infrastructure of a large enterprise, but it still has vital business information and applications which are as important

to the business as any other valuable asset such as plant or people.

For your business to operate at peak efficiency your employees need access to these information assets and applications at all times and wherever their jobs require them to be. Without reliable access they can't serve your customers. And if you have any form ►

Some of the information assets your business probably has:

- Customer database
- Product database, pricelist and web ordering system
- Accounts, payroll and other financial data and applications
- R&D/product development data and collaborative applications, such as SharePoint or Notes
- Market intelligence models and marketing collateral
- Patents and other intellectual property
- Communications applications, such as voice, email, instant messaging and video
- Data and communications archives



The technologies deployed to keep virus and hackers out of a company's systems are only two aspects of a much bigger security picture



of online presence, from simple contact information to more sophisticated online ordering or self-service systems, then customers, suppliers and other business partners expect to access these from any location on the globe and at whatever time suits them.

Furthermore, national government and EU regulations on business continuity increasingly demand that companies can continue to operate even in adverse conditions. All this adds up to a requirement that companies' systems are resilient and reliable, not just secured against virus infection.

Data in transit

In fact, your business information and applications are probably more valuable than the infrastructure that carries them. The challenge of security is to protect your infrastructure in ways that keep data and applications safe, and to make sure data is protected when it's in transit and when it is accessed by remote or mobile employees.

For all businesses, strong information security technology only works if employees are trained to use it habitually. But there are also a number of security challenges faced by mid-sized organisations.

For example, analysts estimate that up to 70 percent of critical data resides on personal hard drives and isn't backed up frequently, a strong argument for automated PC backup services.

Even if your organisation is disciplined about back-up, all vital data and applications may reside on one or a small number of servers, creating a single point (or small number of points) of failure. If your IT department has used virtualisation technology to rationalise the number of servers, then this may be accentuated.

Most mid-sized businesses can't afford to keep a large number of technical



Management issues need to be settled before any technological fixes will work as they are designed to



employees, let alone an expensive security specialist, so there may be a lack of security skills among your IT staff. Threats and regulations evolve, but security atrophies. Thus constant updates to technology, specialist skills and general employee training are required to keep security at an appropriate level.

Lose confidence

Cash-flow considerations mean your business can't afford to be offline for days in the event of a security breach. Besides, business partners, such as customers, suppliers and lenders, and stakeholders,

such as owners and shareholders, might lose confidence in your business or your management due to interruption caused by security problems.

While all businesses have to comply with national government and EU regulations on data protection (for customers and employees), financial reporting and business continuity, these burdens bear heavily on mid-sized organisations that can't afford a large compliance team.

Perimeter

Increasing demand for mobile and remote or home working means the traditional approach to security – building a strong perimeter around the office network – is no longer sufficient.

Security threats don't discriminate on size of business: mid-sized and even small businesses are just as much at risk as large enterprises, possibly more so if they are known to possess highly valuable IP.

Targeting

Cybercriminals are not averse to targeting attacks on specific individuals in companies if they think they have something worth stealing. Security experts say such attacks have increased from one or two a week in 2005 to 78 a day in April 2008 (1). ►



All this adds up to a requirement that companies' systems are resilient and reliable not just secured against virus infection





Threats and regulations evolve, but security atrophies



Given this scenario, ignoring the wider issues of security is not an option for business managers. To do so is to put the business at risk through loss of data and the ensuing business disruption, loss of revenue and reputation and possible fines from regulatory authorities.

The temptation is to instigate an immediate security clamp-down. However, this presents its own drawbacks. Without careful evaluation, spending on security may be disproportionate to the business risk. An ill-considered clamp-down may stifle employee productivity and, once management attention inevitably wanes, an environment of lax security will return.

Employee awareness

Another mistake is to think that security issues can be solved with technology alone. But this will fail to manage the human security issues of employee awareness and training, essential parts of any security policy.

Repeatedly applying reactive technical fixes to perceived or real threats will mean technical, human and financial resources are expended on ad-hoc patches without any regard to the overall security picture or their knock-on effects on the whole system. Security will always be an add-on and never become a pervasive part of the way people work.

Increasing security at the network perimeter alone is not an adequate solution as this will fail to mitigate the risks from mobile and remote access. Furthermore, screening email at the perimeter means Internet bandwidth and storage capacity will be consumed by spam, whereas with a managed security service spam can be intercepted 'in the cloud' before it reaches your network.

In fact, many of the home-grown information security fixes that



Business partners and stakeholders might lose confidence in your business due to interruption caused by security problems



companies can deploy are inadequate responses to today's threat landscape. Consequently, security experts predict that the future of information security is that it will be provided as a service (see Security as a Service).

While this is clearly the future for all companies which can't or don't want to retain a team of information security experts, the temptation to outsource responsibility for all aspects of information security should also be resisted as this, like relying on technology alone, could fail to address issues of employee awareness and training.

Vulnerabilities

Similarly, businesses should be wary of choosing a one-size-fits-all solution from an out-sourcing partner. The solution may leave vulnerabilities if it is inadequate for the size or scope of your business or result in needless expenditure if it is designed for a much larger enterprise.

So how should mid-sized companies respond to the challenges of information security?

First is required a level-headed evaluation to differentiate risks from threats, so that planned security expenditure encompasses the reliability and continuity aspects of information security and can be kept proportional to actual business risk.

Holistic

The focus should be on business management issues not ad-hoc technical fixes, so that your business develops solutions that treat information security holistically and engender an environment of pervasive security.

At the heart of any information security system are the people who access your business information assets and ►

Security as a Service

"More companies are outsourcing their network security," says information security guru Bruce Schneier. "This trend is driven by one truism: there is no other way to deal with the shortage of skilled computer security experts, the increasing requirements for businesses to open their networks, and the evermore dangerous threat environment. For the internet to succeed as a business tool, security has to scale. Outsourcing is the way to achieve that." (2)

"Software-as-a-service and cloud computing herald a seismic shift in the security industry's business model, promising to radically change the relationship between vendors and customers – and reshape the industry," says Information Age journalist JJ Robinson. (3)



Information security should be built in to systems from conception and be a fundamental part of employees' working practices

applications on a regular basis – your employees. Even the strongest security technologies can be breached if the people who are supposed to use it circumvent it. Walk around any office and you will see sticky notes with passwords scribbled on them stuck to monitors.

Awareness of the objectives of information security – reliability and continuity of the business – and frequent updates and training should be a part of

employees' working lives, decreasing the risk of accidental data loss or malicious disruption through social engineering.

The primary objective should be to secure that which is of the highest value to the business, which will emphasise protecting data and applications wherever they are, not just on securing the perimeter of the office network.



Information security needs to be pervasive not an add-on. It should be built in to systems from conception and a fundamental part of employees' working practices.

Tailored solutions

Taking to heart what security experts are saying about the logic of buying security as a service, you should look for partners that complement in-house resources and skills with tailored solutions. That way you can free-up

technical resources for tasks which add value to the business rather than tie them up in routine security patching.

So, is it possible to remove the fear-factor from the information security debate? Yes, most definitely. Information security is about more than anti-virus and intrusion protection: it's about being confident that your company will always be open for business.

Mid-sized businesses face the same threats as enterprises but with considerably fewer resources, therefore it makes sense to look for a partner who can provide the skills and technology which the mid-sized business needs. ■



Security is about being confident that your company will always be open for business



Questions to ask prospective suppliers

- Does the supplier have a track record of working with security-conscious customers, e.g. financial institutions?
- Is the supplier ISO27001 certified?
- Can the supplier cover all information security aspects including reliability and continuity or is the offering limited to protection?
- What degree of monitoring can the service provider offer in terms of availability, restoration time, response time and problem-resolution, and at what cost?
- What level of service can the supplier guarantee for internet and data connections? Does this match your business need for, say, 24x7 connectivity?
- Can the supplier work with local integration partners?
- Can the supplier continue to provide service and support as the business grows?

For further information www.colt.net.

(1) See <http://www.message-labs.co.uk/intelligence.aspx> 2008 Annual Security Report

(2) <http://www.vnu.co.uk/crn/comment/2241727/panic-pass-argument-outsourced>

(3) <http://www.information-age.com/channels/security-and-continuity/features/1017327/the-devolution-of-security.shtml>