

# Handing over the keys

Assuming your house is your most valuable asset, would you be willing to hand me the keys and have me look after it for you? Not that keen? Well surely some charity executives could be excused for feeling that that's effectively the business proposition behind outsourcing the protection and security procedures around their ICT (information and communications technology). After all, if information on donors and members is an organisation's primary asset, why take the risk of losing that by placing it in a stranger's hands?

"There's a natural reluctance on the part of a lot of charities about this," notes John Tate, IT adviser to the Charity Finance Directors Group. And there is also a contradiction, in theory, that a lot of these services run over the internet, not classically regarded as the most bullet-proof of secure systems itself. "There is a definite question mark here in customer minds," confirms Tate. "How much data and traffic can be interrupted and information seen by those who we don't want getting access?"

Nonetheless there's growing interest in what's known as, in one of the technology industry's less felicitous acronyms, MSSP – managed security services provision. This is where third parties offer to host not just an organisation's online presence but also act as the guardian of its network. This can take the form of a range of services such as software to block spam and viruses, to intrusion detection and firewalls to 24x7 monitoring of all traffic. And there are also activities around surveillance and monitoring of staff IT access. Indeed in August last year, IT analyst firm, Yankee Group, went so far as to predict 90 per cent of all IT security could be run by people who don't work directly for the real owners of the protected data by the end of the decade.

The solution to the apparent contradiction – that outsiders want to

If you think the idea of outsourcing your IT security seems a counter-intuitive, risky proposition, then you're probably not alone. However, Gary Flood finds that there are some definite benefits to going down this route, including access to state of the art defences without the vast expense of providing them in-house

protect your invaluable data by using the web – is that there's clearly a difference between the public, surf and shop, internet and the kind of networks experts in secure communications utilise, mainly by hardcore technologies like SSL (secure socket layer) and VPN (virtual private networks). These create 'tunnels' and other ring fenced patches in the web's infrastructure that companies can work with as securely as the proprietary networks of old.

At least that's the claim of firms like Cybertrust, whose director of product management, Bart Vansenant, told Charity Times: "Most organisations we work with realise IT security is important, but struggle to mobilise the resources to do it all themselves. Companies like ours offer the resources and expertise that only the very biggest customers could buy for themselves."

That's a reference to the perception that MSSP is usually for the largest players only. As far back as 2001 IT market watchers, IDC, published research saying it is larger organisations that are more comfortable outsourcing their security functions than their small and medium-sized counterparts, and that doesn't seem to have changed much since.

Or has it? While not a security specialist like Cybertrust, another software company, Winweb, claims all sorts of companies should be investigating IT security outsourcing. "At the end of the day it's a question of belief – if you think your data is safer in your office safe or some dedicated system in your office, or in a secure remote location full of the latest technology safeguards. We provide our clients things they just couldn't afford on their own, such as data backed up on to RAID5 storage, which believe me is horribly expensive, but we can manage it because we're getting the economies of scale to make it

## IT Security Outsourcing Tips

- Define the elements of network security you want to outsource. Common options include: perimeter security (managing and updating firewalls); penetration and intrusion detection; email and web-content filtering to better deal with spam, malware outbreaks and inappropriate use of office resources
- Only choose an outsourcing partner who can advise you on how relevant these services really are to you and put together an outsourcing package that meets your specific security and financial needs
- Then evaluate the provider. Try to meet with the company at their offices to see how they manage their operations and provide their services, and get references from other clients
- Then and only then hammer out the all-important service-level agreement (SLA) which spells out the terms of the contract, including what's covered in the outsourcing agreement, what's not covered, and delineating specific processes for security breaches, reaction times and repair times
- Also get details on commitments to systems availability, uptime, rule changes, patch deployment and issues such as how long until you are protected once a virus has been identified. Sensible negotiation between you and the MSSP should result in a good SLA that will eliminate most fears of making your company's sensitive data available to an outside party
- But don't rest there – have regular meetings to keep up to date and get feedback such as reports on updates deployed, on spam stopped, or on vulnerabilities identified
- Finally, timetable regular (e.g. quarterly) review meetings with the SSP to go over any service or security issues and discuss them in open forum

Source: Network Defence

worthwhile," says its founder and managing director Stefan Toper. "We have eight IT security professionals on this full-time, with two firewalls and all sorts of other weaponry; also all the data is at big data hotels in more than one country so that if one burns down it's still safe."

Toper's firm offers these kind of facilities not because it's a security shop but is instead a provider of software as a service (a practice previously known as ASP, or application service provision). Like bigger rivals Netsuite and Salesforce.com, Winweb users effectively rent applications over the web rather than purchase the servers and licences as they used to, and it works with charities including the Prince's Trust doing so, he says.

"What people need to realise is that though you're not doing all the IT security any more you still control

it," says Cybertrust's Vansenant. "Companies struggle with managing and interpreting the results of all the sophisticated IT monitoring and intrusion detection equipment they may buy. What providers like us do is act as middle men and filter all the information – you are the one who decides what to do when we contact you."

And bear in mind, though the MSSP vendors don't customarily spell it out, that you are still liable for any security problems and reactive measures if needed. Still, as organisations start to work more and more with net-based technologies, including charities, offloading some of the burden of policing all this kit does seem sensible. "MSSP is being used in many organisations now as managers start seeing that buying lots of security products does not equal being secure," suggests Vansenant.

In terms of risk management, then, what is the most sensible approach to IT security outsourcing? Avoid it for the time being or go for it fully? Tate suggests a middle way that could appeal to the responsible charity executive: "It's the usual question of all outsourcing – look carefully at what you can afford to keep in-

house. That can mean evaluating the amount of resource you'd have to dedicate to doing all this yourself; is that money best spent elsewhere? Therefore we would recommend selective outsourcing, a mixed strategy where you work with others only where it makes the best business sense."

Whatever you decide to do your smartest move could well be to pay for at least one

external bit of IT security consultancy; a security audit.

Someone else is much more likely to find the gaps in your city walls than you. Though well short of commissioning an MSSP contract, it could outline whether you really need such a partner or not.