

To print: Select **File** and then **Print** from your browser's menu

-----  
This story was printed from ZDNet Asia.  
-----

## Securing all fronts

By Penny Jones, Technology & Business magazine, Special to ZDNet Asia  
29/4/2005

URL: <http://www.zdnetasia.com/insight/network/0,39044847,39227786,00.htm>



The start of the 21st century has redefined the word "security". Countries go to war for it, constituents vote as a result of it, and companies are learning that to stay safe, and protect valuable assets in these highly technological times: with anxiety increasing in all walks of life, security has become a hot topic, and how it is managed can mean more than just bucks for a business -- reputation, trust and, in-house stability can all rest upon it.

But managing security can be a big headache, and it can be easy to get wrong, especially when basic perimeter security is not enough. Attacks from inside the business are growing and the complexity of the business environment is changing with globalisation. The ability to work remotely, and new technology being designed to link aspects of operation, raise new issues for what was once deemed a simple procedure.

An unprotected firewall can open up thousands of doors for hackers wanting access to your business operations, and spam is constantly being slammed for the thousands of employee hours it can cost each year. Add to this the growing issue of lost business due to down-time, and the ethical issue of keeping your clients safe, and it becomes easy to see why security is no light topic.

Frost & Sullivan analyst James Turner says one of the main reasons the nature of security has had to change is that hackers are becoming much more money-hungry, and extortion and identity theft are becoming a lot more common.

"As capitalism consumes the world, the hackers are coming around to the market's way of thinking and they are looking for their own piece of the action," Turner says.

"As a result, we are going to see an increase of law enforcement on the Internet. Companies are not only going to have to be secure for their own sake, but secure so they can adhere to the new ways of doing business."

So in an effort to erase anxiety, the high cost of security training for IT staff, and company liability, more and more companies are looking to managed security service providers (MSSPs) to manage all or part of their security processes for them. Analyst firm The Yankee Group estimates that by 2010, 90 percent of security operations would be outsourced -- in the US at least.

Services can range from patch management for a particular product, to management of your network's entire security architecture. The companies that we spoke to for this article offered services in the following areas: network intrusion detection and prevention, host intrusion prevention, vulnerability assessments, patch management, firewall and VPN management, and e-mail monitoring for protection from viruses and spam.

Lorenzo Modesto, general manager of MSSP Bulletproof Networks, says a complete outsourced security solution will start with the infrastructure. "You will generally hand this out depending on the skills set and infrastructure you will, or won't, already have in-house," he says. "Managed network security is about prevention -- locking things down so that the managed security provider is not having to chase holes in your system all the time. This is why you start with what is physically there, then determine what requires outsourcing."

The service itself, he says, is all about managing this infrastructure: putting out alerts at times when weaknesses can be found, monitoring how well the infrastructure is working, tuning false positives, and preparing an incident response when a security breach is made.

### Benefits

When a good MSSP is employed, a company should be able to expect constant monitoring and management of both internal and external network operations, depending on the services assigned to your provider. The idea is that as a client, you should rest easy knowing a team of experts is monitoring patch updates and keeping up with world security trends.

However, like most outsourced services, companies will not be able to hand over their liability in regards to security to the provider. Modesto says what IT staff will be able to do though, is show higher management that they have taken big steps to make their company secure. Other benefits of handing over the lock and key are glaringly obvious, he says.

"Cost would have to be the biggest one, on top of expertise. You can have some tough service level agreements (SLAs) written," Modesto says. "But every security provider will tell you that security is one thing that can never be 100 percent assured -- you simply can't guarantee that. Having a managed security provider is all about minimising exposure and managing security effectively -- something a lot of businesses cannot afford. For good security your infrastructure needs to be managed by someone with the time and the right tools and skills set -- things that when dealing with security, are not cheap."

Australian e-mail security penetration tester Neal Wise, partner at Assurance.com.au, agrees. He says as far as labour and costs go, making your security problem someone else's can be a very attractive offer. "There are perceived cost savings with managed security, as security personnel are not cheap, and you get round-the-clock service—that is obviously the number one benefit in this time when so many threats loom," Wise says. "But you have to manage the security relationship right as no one is going to understand your security needs better than you are."

Wise says managed security increases its attractiveness 10-fold when benefits such as constant patch updates and the securing of Web applications can be seen. "Web applications are the most direct way for attacks to occur, and most businesses realise this," Wise says. "If someone wants access to a system, no matter how good the managed security is, they will find a way of gaining it. The benefit of managed security services that work properly is the response time to this."

Melbourne-based MSSP Dimension Data has clients in Europe, the US, and South Africa. National security manager Neil Campbell says in all continents, cost is only part of the reason his clients choose managed over in-house models. "Most of our clients do not have the resources to deal with security properly so cost is one reason they turn to managed security, but a lot of people are also tempted by the fact that you are handing over that part of the business risk to someone else," Campbell says. "Many businesses find it is quite difficult to attract and maintain security personnel, especially if operating as an SME."

### **Handing over control**

But when should companies consider coughing up the bucks and moving on to managed security? Frost & Sullivan's Turner says: "A business should consider moving to a managed security service provider when they estimate that the risk of loss outweighs the cost of the service, and the cost of maintaining the in-house skills needed to manage it."

"If your business is in any way reliant on connection to the Internet 24x7, then ideally you either have 24x7 security staff or an MSSP. The MSSP can provide good network security much more cheaply than most companies can provide it themselves because they are the specialists and they have economies-of-scale which make it more affordable," he adds.

General acceptance of managed security may be growing, but reputations of unreliable providers still, to some degree, hold the service back.

Industry cowboys still exist -- there are numerous horror stories of people signing up with an unreliable provider only to find out months down the track monitoring has not been maintained at its promised levels, or that small start-ups are facing insolvency rendering all contracts at risk and costing companies dearly.

Andrew Tune, director of MSSP Network Box, says credible providers are still fighting a negative perception, largely as a result of negative customer experiences.

He says he has spoken with some customers who have disabled their connection to their provider, only to find out the provider was not even aware they had done so.

"This one customer called their provider to tell them they had taken out their security box. The provider said no they hadn't, it was still being monitored. They did not even realise they were no longer monitoring their client's security," Tune says.

He says this is not an isolated incident and companies should beware, when choosing a provider, that they are getting the service they are paying for. Negative incidents have somewhat tarnished the image of the service, but with the right provider, companies should not have reason to be concerned, he says.

"Companies are concerned about loss of control -- but that is really an emotive thing now. You also find IT staff concerned that we are coming in to take over their job, but that is not the case," Tune says.

"We are coming in to make them look like heroes -- so they can say 'here, look what we have employed and look at what it has saved the company, and look how quickly we have had all this implemented'." Sydney-based Pure Hacking has penetrated the walls of a number of large financial institutions. They say in their testing they have come across both the good and the bad in managed security. Their take on choosing a provider is to find one that can fit all of your direct requirements, and, even better, that specialises in all these areas.

"It is a very specific job," Pure Hacking director Rob McAdam says. "You have to work with people who are really focused on security only. My motto is 'if you believe you require a square peg then you must put a square peg in place'."

### **Weighing it up**

Security software company Sophos resells its products to large ISPs who in turn sell the software as part of a managed service. Sophos managing director Rob Forsythe says he views the general company cut-off for the hire of specialised security staff to be businesses with less than 1000 employees.

"A larger enterprise would buy our product direct, and manage their own network which would allow them greater internal flexibility, but a smaller one, to have the same level of security, would have to look for outsourced flexibility," Forsythe says. "Then you also have the difference in cost in relation to having the capital expenditure per month, instead of the outright cost and total cost of ownership."

Assurance.com.au's Wise says a company must carefully manage the level of risk they are at -- security wise -- before putting out the cost for managed security, however.

"Security is something most organisations can afford to have, but they don't always realise that you get the best bang for your

buck so you really want to know what it is you are needing," he says. "Like in most industries there are plenty of shonky salesmen out there, you have to be really careful you are getting a reputable operator for your money. You need to really ask what it is you want from your service: if they have around-the-clock appropriate staffing, if they have more than one operating centre, if they have good customer references and what sort of audits or reports they will offer."

Security is a big concern, but trusting your security, in the first instance, must be an even bigger one to get it right. Plenty of companies have been through the trial-and-error process of doing security in-house, and that of selecting a credible security provider.

"Selecting the right person is even more important than getting your infrastructure right," Bulletproof's Modesto says.

"You have to get a good feel for a company, from the top down to the bottom. Do your homework and never underestimate the selection process. A good provider should be able to provide ethical resources in the pre-sales process and should allow you to talk to their tech people as well as the initial supplier to get a good idea of how the two groups interact."

### **SLA security**

Like with most outsourcing initiatives, your service level agreement (SLA) between yourself and your provider can either be your saviour, or the bane of your existence.

The SLA could very well be the most important part of your relationship with your managed service provider. It will define the roles your provider has in regards to your company, and what you should and should not accept for your money.

Traditionally, your money will ultimately drive what you can and can't have in your SLA. The more you pay, the more customisation you can expect.

Standard SLAs, for instance, may simply determine how many changes you can have within your business for firewall protection under a particular cost. But no matter how small your security objective, the SLA must be clearly identified.

Frost & Sullivan analyst James Turner says contracts are one of the key areas of concern with any outsourcing venture. "No one wants to spend six months arguing over who is responsible to pay, say, for hardware maintenance. Just like with all good business projects, ownership must be attributed to each task," Turner says.

For security, the key areas you should be considering when you write up your SLA are:

- **Security management** -- how will your security be managed?
- **Monitoring** -- what level is acceptable to both parties?
- **Incident response** -- what response time is acceptable and processes carried out in doing this?
- **Documentation** -- what audits will take place and what feedback will you receive and under what time frame?

You can also add in security tests, penetration exercises, authentication and access control and auditing if suitable. But remember, with outsourcing, each service comes at a cost.

Modesto, and other providers, believe managed security will become all the more critical in coming years as companies place increasing importance on technological advancement and information protection.

With that in mind, companies must be ready to do their own homework before they choose their managed security provider as it is one thing to baton down the hatches to the outside world, but yet another to throw away the key.

### **Nintendo plays the security game**

Keeping costs down and attracting qualified security staff were problems for Nintendo Australia. When it received a directive from head office in Japan to start analysing the logs from their CheckPoint firewall or a possible replacement Netscreen appliance, Nintendo Australia IT manager Peter Stroud was concerned by the expense of the project, even though he could see it was a good step.

"We thought it was kind of like shutting the gate after the horse had bolted -- we were going to have to spend a lot of money but we would only have the information analysed a week after any violation," Stroud says. "We thought if we were going to spend the money on expensive software we would also look around to see if we could find something that did intrusion detection and prevention, which led to us deciding we may as well outsource the whole thing."

Price-wise, Nintendo looked at a variety of options and the most expensive quote was AU\$30,000 for the installation of equipment only, and another AU\$30,000 a year on top of this for the 24x7 maintenance and support of that, which is too much for the small company of only 60 local staff.

The gaming company ended up going with Network Box, an MSSP specialising in complete managed security. "We chose the Network Box because, for about AU\$1200 to AU\$1500 a month we were able to get our security at half the cost. We can restrict site access for staff, we have no hidden costs, we have 24x7 support," says Stroud.

"Responsiveness was our main concern. It did not take us long to realise that [Network Box] could actually do the job much faster than we could. The only negative aspect is that we really do not know what is going on within the box. We had been attacked by a hacker who was using our bandwidth before, but since going on to managed security we have had no attacks at all."

### **Queensland company saves with security**

Queensland-based integrated engineering and services provider Thiess approached IBM just over a year ago about problems it was having with "ridiculous" amounts of spam, viruses, and pornographic e-mails taking up valuable employee hours and leaving the company at risk of attack.

"We could see the huge amount of time it took employees to sort unwanted materials from regular business e-mail, as well as the strain it was placing on bandwidth of our corporate network," says Thiess infrastructure supervisor Richard Moran.

Thiess went to IBM, a reseller of MessageLabs managed security services, signed on for anti-spam, antivirus, and image control (to block distasteful Internet sites) services. As part of the service, Thiess' mail delivery and Internet access was reconfigured to pass through MessageLabs' infrastructure before making it to the desktops of Thiess employees. IBM provides all the service's 24x7 support.

"The most effective solution for us was one that eliminated e-mail threats by sitting outside the boundaries of our corporate network, filtering all e-mail prior to their delivery by acting as a first line of defence," Moran says.

"Spam has largely gone away now and the viruses are no longer a problem -- we now get about a quarter of the amount of e-mails we once did so it eliminates our risk and saves us time and in the end, money".

**This article was first published in Technology & Business magazine.  
Click here for subscription information.**