

# Cover Feature Security

## DIVERSIFYING SECURITY

Resellers need to consider multiple vendors as IT security changes

By Lilia Guan

**A**NTI-VIRUS VENDOR Tumbleweed has released its findings on the five pressing security threats that will emerge or continue to plague IT security in 2007. As anticipated, data leakage concerns and continued growth of profit driven spam will top the list this coming year.

Dr Taher Elgamal, chief technology officer at Tumbleweed, says the spam problem will continue to grow and be increasingly profit-driven.

"Spammers will continue to exploit new ways to circumvent spam filters, such as using video and audio files to avoid detection. We will also see data leakage become the biggest issue in 2007," he says. "Most organisations do not realise how much data is travelling outside the enterprise, usually via unsecured methods.

"As a result, desktop encryption will become a mainstream defence mechanism and content security will become more sophisticated to address this shift towards

data protection, monitoring both inbound and outbound traffic for multiple protocols."

Most spam will be focused on the categories with the highest potential for profit. For example, 60 percent of spam at the end of 2006 was for stock tips or drugs – areas where there is a clear profit motive – and this will continue to grow in 2007.

Recently Australia was hit by a fake political spam announcing Prime Minister John Howard was having a heart attack. Then another spam announced the Australian cricket team was fighting for One Day rankings, proving that spammers will continue to find new ways to circumvent spam filters. For example, spammers will seek to randomise images to evade spam filters to penetrate inboxes.

Set to gain more steam in 2007, the 'logo gibberish' spam is a recent example that uses legitimate graphics within the email to confuse filters.

This year will see hackers and spammers also trying to take advantage of audio and video files, using them to deliver viruses, mask and deliver spam messages and generally avoid detection by conventional spam filters.

Botnets are armies of hijacked computers used to deliver spam and these will remain an issue in the coming year. The botnets allow spammers to deliver thousands of messages while avoiding reputation filters that block known spammers.

With this type of threat evading all areas of an organisation, resellers need to look at which solutions best suit their customers to prevent an attack occurring. General consensus in the industry seems to be that there



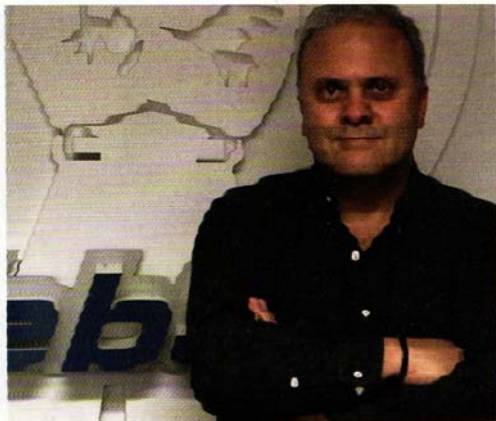
is no one solution that will protect the network and the desktop.

"To sell security, resellers need to keep the IT systems together and forming a big puzzle," says Tom Piotrowski, managing director of niche security distributor Unixpac. "Keeping constantly educated on how new technologies interlock with others is relatively easy to follow."

Lagis Zavros, COO of Internet reporting software vendor Webspy, believes resellers need to take a more holistic view of the whole security market. The Internet and its tools like instant messaging and YouTube have taken the issue of compliance to a board level. Managers have become much more responsible, especially with compliance and mitigating risks.

"There is a trend towards being able to report to provide evidence with what has happened for legal compliance. Internet-based communication like frame relay, ATM and Internet-based VPNs for VoIP has opened a lot more holes for organisa-

WEBSPY'S ZAVROS:  
Resellers need a  
holistic view



**"Spammers will continue to exploit new ways to circumvent spam filters"**

LINKSYS<sup>®</sup>

A Division of Cisco Systems, Inc.



tions. There is a trend for vendors to come up with newer products," Zavros says.

**Changing face of security**

Dominic Whitehand, managing director of Whitegold Solutions, believes one of the biggest things that niche distributors might see is a lot of the resellers in deals were they provide a multi-tiered portfolio to their customers. These resellers will look at an organisation's gateway and offer customers one product then go with a completely different anti-virus vendor across the whole network.

"These resellers will typically go into security and ask networking people like Whitegold which vendors are complementary to each other. We have vendors working with us that offer multiple solutions including Secure Computing, with a whole range of products from UTM to URL filtering, Barricuda and Fortinet," Whitehand says.

Joel Camissar, managing director of

**"To sell security, resellers need to keep the IT systems together and forming a big puzzle"**

anti-virus vendor Websense, says it is "very interesting" how things work out in the security market. About 10 years ago multiple vendors and partner organisations used to sell single security portfolios.

"Once, anti-virus technology meant cheaper licences and resellers felt customers could be better protected. However, this has all changed and organisations are now saying the product I have is not working and threats are evolving," Camissar says.

"Security resellers can't keep pace with what's out there other than specialising in one area and putting their eggs in one security basket, meaning resellers are leaving money on the table. There are a range of solutions that are complementary to each other and they can't just say that this one solution they have is the best – they need to be flexible to meet customer needs," he says.

The end user is becoming savvy than ever before and Camissar believes that servicing is just one

part of the total package they expect. Any customer can do a Google search about products and in a matter of a few hours can become an expert and approach their reseller about product XYZ.

"I personally think security resellers are struggling with the technologies which are best of breed and as a result there is a tendency to become opportunistic and are led by what a customer wants rather than what they require," he says.

As the changing landscape becomes more confusing it is important for resellers to be more careful about so-called leading technologies. Unixpac's Piotrowski agrees that end users are doing their homework about security and resellers are being influenced by what an end user wants.

**On the mind of resellers**

AVT IT is an IT systems integrator based in Melbourne. Its focus for the past 15 years has been to provide the SMB market with security managed services and networking data recovery for an organisation with sub-1000 seats.

Jason Price, technical consultant at AVT, says its customers are starting to demand enterprise security solutions.

"We are finding a lot of vendors trying to be the 'be all and end all' for example for a reseller," he says. "One example is Trend Micro, which has products ranging from anti-virus to spam but as a reseller it's important to engage a number of different vendors as opposed to what a vendor wants you to sell," he says.

Price says resellers in the IT



# Cover Feature Security

market are in two mind-sets about selling. One set takes the vendor of choice and makes it fit; however, companies like AVT offer complementary products.

"I attend a number of seminars and think if you pay attention to the different kinds of threats that are out there, resellers need to take into account threats are now coming from different areas and are commercially different," he says.

Price believes that back in the day when a virus was written by a 16-year-old, it was for fun and there were no monetary gains to be made from it. Now it's all about making money from threats.

He also says that SMB customers are aware of security threats and at this point in time they just want to make sure they have their firewall and protection in place.

"They aren't aware about what they need for threats coming from the Web. People are trying to hack into their network. We are also finding organisations are no longer a single site; even smaller organisations can have multiple sites running across multiple networks with WAN intricacies," he says.

This is where a multiple solution comes in handy because a lot of vendors only have one particular desktop product and may know nothing about WANs, as vendors that sell WAN products know nothing about a desktop.

Craig Flowers, pre-sales manager at Express Data, believes one vendor can't give end users total security — for example, just because they have RSA doesn't mean they won't

| FIREWALLS: TOP 3 BEST-SELLERS | 2006 MARKET SHARE | 2006 MARKET SHARE CHANGE |
|-------------------------------|-------------------|--------------------------|
| CISCO SYSTEMS                 | 37.7%             | +19.9                    |
| SYMANTEC                      | 34.6%             | -21.0                    |
| CHECKPOINT                    | 15.2%             | +5.7                     |

Source: The NPD Group/Distributor Track

have anti-virus and spam products from other vendors. "It's been going on for some time and will continue for a lot longer as there are less vendors to choose from because niche players are being subsumed through consolidation," Flowers says.

Continuing the IT security of a business goes beyond the office. Flowers believes you don't have to be inside the office as attacks are rife and can occur beyond the traditional four walls.

"The arrival of the [cruise ship] QE2 caused the City of Sydney to come to a standstill. The APEC conference will also bring far worse problems to Sydney. Resellers will be out there thinking about remote access and security and they have to make sure firewalls are in place," he says.

"This is where the need for education to prevent an organisation breaking down is important. As a distributor, Express Data doesn't favour any one solution, we educate resellers about the right vendor. Larger resellers out there will have access to five or six key vendors. Why should it be any different for the smaller guys?" Flowers says.

## Correlating the products

Nick Verykios, marketing director of Distribution Central (previously known as Firewall Systems), believes organisations should be worried about a prevention policy, which relates back to a security policy with technology overlays that is not made by security vendors.

"The security landscape is going to be about the securing of infrastructure versus the network versus the end user," Verykios says.

"It's not just a vendor doing everything, it means running four to five applications out of 20," he says. "However, the end user will say they want central management and throw it on a box run dual layer with anti-virus on one gateway."

Verykios goes on to say that it is very different from the past vendor mentality of 'I have built something — you need to work around what

I have built'. He says the reseller is being asked, 'Can you get this and that product from the end-user?'

"These guys are saying we don't even know what the threats are and you can't detect the unknown then prevent it from occurring in the first place."

Verykios explains that major integrators and any resellers have a multiple vendor approach for that reason — to prevent an attack.

"Different vendors can create the perfect solution for resellers to go out and sell as one holistic solution. It is a lot better than them going out and saying their one vendor product is the best," he says.

"Resellers can't keep it stale because security has changed and end users are getting information which is readily available to them so they will end up one step ahead of the reseller."

There are some vendors out there that acknowledge that they are not in a position to do everything and are realistic about resellers having a multiple vendor approach.

Unixpac's Piotrowski says people do realise they need to cover all holes in the security space. However, he also believes that suppliers don't realise patching it with multiple vendors will not to solve all problems.

"Sometimes it can be a case of the more you have the more you have to watch and correlate. When you install various devices on the network the reports that are generated can turn out events that have happened into a false positive," he says. "Something is happening but not necessarily reported because you have to watch out for something else happening on the network and correlate the information."

Piotrowski believes as security matures more technologies will be needed to view from a management perspective how the network is going. Many devices aren't working in sync to achieve a certain level of security, which is important to establish whether or not everything

**"These hackers are driven by profit and that is the far-reaching motive"**

Distribution Central's Verykios: Multiple vendor approach to prevent an attack





Websense's  
Camissar:  
Flexibility to meet  
customer needs

is working correctly.

"People are concerned and even in big enterprises things still happen, that's why you have banks armed to the teeth because they are constantly subject to attacks. Resellers must evaluate their customers' technology because there is a certain life span to products," Piotrowski explains.

"You can't buy a firewall and assume it will protect you today because hackers never sleep, so they will try to bypass all security products. There needs to be a continuous flow and integrity to a customer's network."

#### Future of selling security

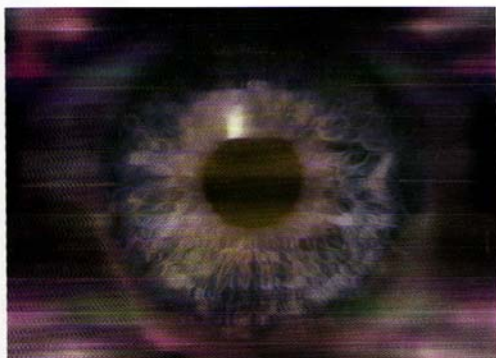
Resellers need to focus on providing their customers with a holistic approach as part of their package.

It's no longer enough to say 'we can offer services', and vendors have been dangling the service carrot for many years. There are educated customers wanting to find out about plugging all the holes in their IT security. Right now the security landscape is all about bringing out the best of breed, which also needs to operate cohesively together – the more ease of use, the better the products are for the end user. If resellers spend all their time fixing

#### "Government organisations said that no anti-virus vendor had a filter for the trojan horse virus"

their customers' computers, when will they have time to up-sell other areas of services they have available?

When Websense's Camissar speaks to resellers he finds that foremost in their mind is the gap between what anti-virus vendors are able to



#### CHANNEL BEST-SELLERS: SECURITY



By Kevin McLaughlin

Cisco Systems has long been a familiar name in firewalls. But in 2005, the networking giant watched while competitors ate its lunch. Last year, Cisco turned the tables.

According to The NPD Group/Distributor Track, which monitors the US dollar volume sales of high-tech products through certain major distributors, Symantec held a 55.6 percent share of the firewall segment at the end of 2005, compared with Cisco's 17.8 percent share.

Solution providers point to two key events as the impetus for what amounted to a dramatic turnaround last year. In June, Symantec said it would decrease its investment in security appliances, including the Symantec Gateway Security appliance line, which includes firewall capabilities. Then, in July Cisco added two new models to its Adaptive Security Appliance (ASA) unified threat management series, which also includes a firewall.

In the wake of these events, Cisco's US dollar volume share for firewalls leapt nearly 20 percentage points in 2006 to 37.7 percent, overtaking Symantec's results, which slipped 21 percentage points to 34.6 percent, the NPD data shows.

A big reason for Cisco's firewall market leadership is the trend towards companies looking to consolidate multiple functions within a single appliance, which has helped fuel sales of the ASA line, said Steven Reese, security practice manager at Nexus Integration Services, a US solution provider.

Now that management scale has become an operational function, simplifying management of security infrastructure is many companies' primary goal, he said.

Steve Pettit, president of Blue Spruce Technologies in the US, is seeing "a lot of customers" upgrading from Cisco's PIX firewall to the ASA, and he thinks the ASA series is also taking market share away from Cisco competitors including Symantec and Check Point Software Technologies, which was the third best seller in this segment with a 15.2 percent share.

Cisco's SmartNet support is another reason behind the vendor's recent firewall market gains because customers like having an entire organisation that works with them to support complex solutions, said Gary Berzack, CTO of Cisco partner eTribe, New York. □

capture and what threats are out there. "I had a day of meetings in Canberra in March with Government agency organisations and they brought up the fact that no anti-virus vendor had a filter for the trojan horse virus. None of the contact filtering vendors were protected from the horse because new forms of variants were bypassing multi-layers of defence threats," says Camissar.

"The threats were continually evolving and it was becoming harder to keep up with the hackers."

He believes because of this environment it is worth resellers asking vendors about complementary technologies being adopted. Resellers don't want to look at vendors that won't be around for the long run because there is a level of complexity that has come back to the security market due to the Internet. A recent report issued by Yankee Group for the Symantec, RSA, Cypher Trust and Websense, states that 79 percent of all threats were Web-based.

"These hackers are driven by profit and that is the far-reaching motive in the hacking community; they have changed the rules of the

game and it has become harder for traditional technologies to keep pace with the threats. Resellers need to continue to relook at their portfolio, otherwise they leave the door open for other resellers to come in," says Camissar.

While local organisations are busy with securing their computer, AVT's Price says it is never too late for SMB resellers to look at securing data within an organisation – after all they are the front line fighters for many sub-1000 seat organisations.

"A company's need to access data from anywhere can put valuable data at risk. We only have a few customers that have engaged in locking down information. It's never too early to look at these types of issues because an organisation's data is its bread and butter," he says.

"Once compliance issues and regulatory issues come to Australia the way they have in the US, organisations will have no choice but to make sure their company information is secure, wherever it is. However, a lot of resellers at the moment are ill prepared for it," Price says. □