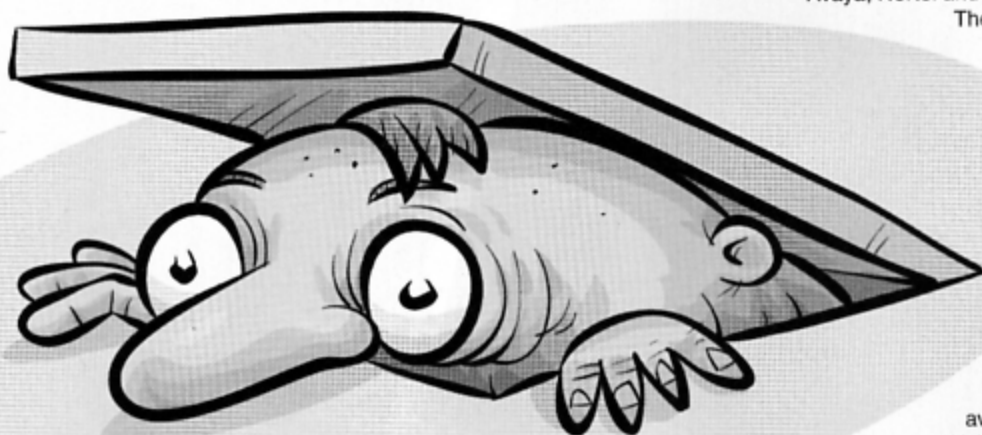


## PRODUCT FEATURE



# Batten Down the Hatches

With the popularity of VoIP services increasing in both SMB and enterprise markets, the risk of crippling cyber threats is looming large. ROB IRWIN reports on some of the emerging concerns and how resellers can help customers avoid a meltdown.

**2006** was undoubtedly the year of VoIP. Wherever you looked, new VoIP installations were making the news.

What goes up must come down. Market analyst, IDC, reports VoIP market growth will slow down this year to about half the 2005 and 2006 growth rates.

Don't go ringing any alarm bells yet, however. The good news for vendors and the channel is that IP phone and IP PBX revenue is expected to continue growing as larger sites start to come on-board. IDC figures suggest 14.49 per cent growth to reach \$606.76 million in 2010 with vendors such as Cisco, Avaya, Nortel and Alcatel leading the way.

The total market revenue of Australian VoIP services, including managed/hosted VoIP and IP Centrex, will increase to \$462.12 million in 2010.

### Keep it secure

With VoIP appearing inside an increasing number of businesses, it's become a tantalising target to hackers. As some commentators observe, IT security is an important topic at the best of times, but even more so when the technology in question is replacing the world's most resilient and available communications network.

"VoIP is much more involved than just providing a voice solution that works," Integ Communications CEO, Ian Poole, said. "It's actually part of an overall service which secures the data infrastructure plus any other applications and devices connected up. At the end of the day, it's the end-to-end securing of the network."

The issue of security comes into play with an increasing number of technologies converging on the average business network, NSC Group managing director, Craig Neil, said.

"VoIP security is the biggest question we now get asked about when putting solutions together for customers," he said, "particularly as we're seeing a lot more network-centric technology coming into play; it's not just IP telephones on desks."

In addition to IP phones, applications such as soft phones – software for making telephone calls over the Internet – and the integration of voice into applications such as Microsoft Outlook were creating a whole slew of security concerns as more potential weak links were introduced into network infrastructure, Neil said.

Last year, Sydney-based integrator, Integ, compiled a whitepaper for businesses on major VoIP security threats, including how to identify them and adopting an effective security plan to stop them in their tracks.

The key was to secure all elements affected by VoIP – from the handset through to the desktop and LAN.

"Security remains one of the main issues when people look at IP telephony solutions," Poole said. "It's become extremely high profile now and a wider issue."

Fortinet country manager, Charlie Cote, agreed that as interest rose, the threat to VoIP networks was also growing exponentially, particularly for SMEs.

The kinds of exploits used by hackers and other malicious Internet users to target anything from SMBs to the largest of enterprises can vary from denial of service attacks, spam over IP, viruses and worms, eavesdropping and toll fraud.

"A client of ours was hit by toll fraud, where someone got into the voice messaging system and into the management of the system to call in and call out," Integ's Poole said. "Now, to do that you need to be able to access the password, and password protection is such a simple thing that it could have been avoided altogether."

While attacks such as the one cited by Poole seem more

# PRODUCT FEATURE

← from page 20

of an annoyance than a disaster, Check Point regional director, Scott Ferguson, said some strikes on VoIP systems could prove quite catastrophic.

"All the worms and viruses we've seen in recent times have been capable of taking down a network," he said. "Nowadays when you lose the network, you also lose your VoIP and that's like having your arms cut off. It leaves a big hole in your life."

One area sometimes overlooked in VoIP security is the threat posed by good-intentioned but non-technical staff within the company where the VoIP network resides.

"We find that 95 per cent of faults on VoIP networks are caused when someone inside the company changes something on the network," NSC's Neil said. "You might have a good, secure, reliable network running voice and data and then someone puts some new hardware on it. That's one of the biggest security risks we commonly see in businesses – and it's internal and not even deliberate."

Ferguson pointed out that besides the loss of dollars experienced by a company when personnel are left idle without telephony or Internet access, the lack of essential services, such as emergency numbers, cannot be underestimated when reviewing the value of VoIP security.

Many smaller businesses don't have the on-call IT staff across each and every change to a network, which further compounds the problem of a VoIP attack.

## Addressing the problem

NSC's Neil said that, if done correctly, the key components of IP security can be found in the initial design of the network carrying the voice data.

"There are some great ways to secure a VoIP network. A lot is in the initial design," he said.

Check Point's Ferguson said one example of this design could be ensuring voice traffic always has the highest share of the bandwidth.

"VoIP as an application is time sensitive, while general data can stand some propagation delays," he said. "So the network needs to be redesigned to accommodate the bandwidth requirement for VoIP and ensure that it gets priority."

Vendors were also in broad agreement the channel's role was in working with customers to design networks correctly

and roll out the kind of secure VoIP solution that will work best.

"There are some fundamentals around network design and availability needs that require some high level expertise which many customers don't have," Ferguson said. "One of the services we've seen opportunities for in the channel is proper pre-sales consultancy. And by that I don't mean 'Here's your design,' being sketched on the back of a beer coaster – I mean a proper network being planned and structured."

NSC's Neil said designing and maintaining secure networks for businesses was particularly applicable to the SMB market.

"The big financial institutions, for example, have people monitoring their networks all the time, but smaller organisations don't," he said.

"They're more worried about simply growing their core business and getting on with it, rather than looking after networks which is why companies like us are managing more networks than ever."

There were also emerging security developments, such as encrypted VoIP, starting to expand out from military and defence circles and into enterprise solutions which opened up opportunities for resellers, Ferguson said.

Managing networks allows channel players to add new services contracts to their repertoire, particularly in the face of ever decreasing hardware margins, he said.

"Everyone knows there has been a significant reduction in the margins in selling hardware and software and moving into value-added services is the way to go," Ferguson said. "You can start with the initial deployment of a network and then move into a broader range of managed services."

Integ's Poole said resellers should observe the rising demand for tailored and flexible solutions being requested by businesses and create solutions which adapt to specific customer pain points.

With mobile workers accessing all manner of applications and data from outside a business, channel partners need to design clever solutions to ensure that the number of security holes doesn't open up exponentially and unnecessarily, he said.

## 6 STEPS to safe-guarding a VoIP network:

1. Securing handsets and softphones
2. Securing PBX and call management systems
3. Securing switches and routers
4. Securing LAN and WAN
5. Securing desktops and servers
6. Securing knowledge

Source: Integ

# The approaching threat

The Voice over IP Security Alliance (VoIPSA) was formed in 2005 to create VoIP-specific security resources. According to VoIPSA chairman and founder, David Endler, who is director of security research for TippingPoint, VoIP is susceptible to the same types of attacks that threaten other network applications – and there are potential new threats ahead.

### Q: What new VoIP threats do you see out there?

**DE:** We saw the first voice phishing attack. It looks much like the traditional email phishing attack except that, instead of tricking or inducing your victim to click on a spoofed link to take them to a website, you're actually tricking them to dial a phone number that takes them to a spoofed automated attendant. If I can trick you into calling a number that you think is Bank of America, then I can ask you to enter in your account info and your PIN number and even other verification details. Then the hacker can go in and reconstruct those tones after the fact and use them to access your account.

### Q: What other new threats have you seen?

**DE:** The rest of them are more mischievous or not necessarily as financially motivated. Things like redirecting someone's incoming calls to yourself might

become a problem. Registration hijacking is the way you would do that. The way these phones work is when I take my VoIP phone and plug in, the PBX knows that I am where I am basically by my IP address, and all incoming calls to me go to my office phone.

But if I go on the road and I take my phone or I use the softphone on my laptop, I'll want incoming calls to go there. Registration hijacking is tricking the PBX into thinking that someone has moved and then having all their calls directed to the wrong IP address.

There's also something called an invite flood, which is more for an SIP-based network. This is about making someone's phone ring off the hook. It's like a flooding attack on the application side.

### Q: What can you do about that?

**DE:** Enabling encryption and authentication on the

VoIP side helps. That way you can't necessarily spoof messages to the PBX as easily.

### Q: Do general network attacks affect VoIP more than other applications?

**DE:** There are measures you can take to mitigate against denial-of-service (DoS) attacks or distributed DoS attacks. Within an enterprise without VoIP, you may not feel the pain as much, because an email that you sent might arrive a few hours later. VoIP is not as forgiving. It has very strict QoS requirements, so a distributed DoS attack can cripple your VoIP network so that calls coming in are unintelligible or you think your phone system isn't even usable.

### Q: How steep is the learning curve for securing VoIP?

**DE:** We looked at Cisco, Avaya, and Asterisk, and we looked at some of the softphone technologies that have the potential to permeate into the enterprise – things like Skype, MSN. What we found is all of these systems are securable, but they do take some knowledge to get them to that point. None of them come installed by default out of the box in a secure manner. Disable services that aren't really required. Many of these VoIP phones have Web servers on them and things like Telnet and FTP. A lot of these phones are almost like minicomputers. You really need to apply best practices that you would with any other technology.

– TIM GREENE