What you can do to minimise the risks

There are a range of actions VoIP providers can take to secure their networks and protect their customers.

The first essential task is to adopt the same sorts of security measures used on a data network and apply them to your VoIP systems.

Locked-room physical security to prevent hackers from accessing your equipment and secure passwords on management interfaces are basic steps to discourage unauthorised access.

As with any IP platform, the choice of security measures will be different for individual providers, so you may consider seeking expert advice from a security specialist.

Basic security measures like firewalls, encryption, anti-virus software, intrusion detection systems etc should all be considered at vulnerable points within the network. Also, because of the multi-provider nature of many VoIP services, you should consult your alliance partners about their vulnerabilities.

You should also consider the needs of your customers and whether they require education about using security tools such as anti-virus software and firewalls. Some end-user equipment may have firmware upgrades that can be applied or software patches that can be installed. You may wish to supply these fixes to your customers or at least advise of their availability.

Keep sufficient details about calls and charges in order to answer queries from customers and to investigate possible cases of fraud. These details should be kept for at least 2 billing cycles to give customers time to detect suspicious entries.

If you suspect illegal activity or detect breaches, you should contact the Australian Federal Police on (02) 6223 3000.

As VoIP becomes more widely deployed within Australian businesses and the community the threat level will inevitably increase accordingly.

The bottom line is that security issues have the potential to cause serious harm to the acceptance of VoIP as a viable alternative to traditional phone services. It is in your interests to act now to address these issues.

For further information on VoIP issues contact Communications Alliance on (02) 9959 9111
or visit the Communications Alliance website www.commsalliance.com.au/projects/voip

For details on VoIP Security issues, see www.voipsa.org

V4 28Aug06

VoIP Security

What you can do about it as a VoIP or Internet Service Provider

COMMUNICATIONS ALLIANCE LTD

Level 9, 32 Walker Street
North Sydney
NSW 2060 Australia

Correspondence:
P.O.Box 444
Milsons Point NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
TTY 61 2 9923 1911

E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507

Why is security a concern for VoIP providers?

As Voice over IP (VoIP) services continue to roll out to Australian businesses and consumers, security is becoming a defining issue.

VoIP providers have an obligation to fully acquaint themselves with the potential security risks associated with VoIP services and to take action that minimises those risks.

In some cases that action may involve locking down your own networks and systems to prevent malicious attacks or theft of customer information.

In other cases it may require you to educate your customers on potential risks or to modify end-user equipment to make it more secure.

Failure to take security seriously will not only harm customer loyalty and turn potential users away from VoIP but it will also open doors for criminals and terrorists.

How secure is your VoIP service?

Whether VoIP is delivered via the public Internet or a managed carrier grade IP network, there are multiple points at which it can be vulnerable to malicious and/or criminal exploits.

Like most IP platforms, IP telephony-related hardware and software contain "design flaws" that would allow an attacker to cripple a network, deploy viruses and Trojans, steal information, eavesdrop on conversations, spam and scam, as well as numerous other acts that range from annoying to extremely serious.

Vulnerabilities exist in the IP telephony protocols, web servers, databases, call processors, gateways, switches and routers.

At the customer end, PCs, servers, softphones and other devices are also potential sources of concern.

Skilled hackers and computer criminals can compromise any IP-based platform if necessary precautions are not observed and VoIP is no exception.

Any traffic sent over the public internet is directed over an unknown path through unknown operators. Therefore, it is important to make clear to consumers that absolute security cannot be provided in such cases.

What are the major security risks?

Research conducted around the world has identified a variety of security risks relating to VoIP services. Although they vary in the order of importance, most lists contain the same top concerns.

- **Eavesdropping** on VoIP calls is possible using a number of techniques and this is a concern not only because of personal privacy issues but also because it can allow criminals to steal sensitive information. For people using VoIP to access telephone banking or pay for goods or services with a credit card, this is especially worrying.
- **Denial of service** attacks can cripple a network or an endpoint by overloading it with calls. There are a variety of forms of these attacks but they can all cause disruption and loss of business for the victims.
- **Identity- related attacks** can occur anywhere along the signalling path. The user's identity information can be "spoofed" using a variety of scenarios. Identity misrepresentation is a common element of a multi-stage attack, such as getting "free" calls (charged to someone else) and Phishing (tricking someone into giving out confidential information such as passwords).
- **Spam over Internet telephony (SPIT)** is not a significant problem as yet but could become so when VoIP achieves sufficient scale to make it financially viable. Some experts have warned that the volume of spam experienced with email in recent years could be mirrored on VoIP, with voicemail boxes becoming clogged with advertising messages.
- **Viruses** that currently infect computers and clog email networks are just as dangerous for VoIP services. A virus can not only damage the system but can also establish itself on a PC, softphone or network and then open the door to load more complex phone-tapping software from a hacker.