



## VOIP Security Strategy and Assurance

Convergence of data, voice and video over the same infrastructure has cost benefits that can no longer be ignored; a single IP network to administer, and potentially a substantial cost saving in telecommunications.

As Voice over Internet Protocol (VoIP) gains in popularity, phone calls will simply become another packet in your IP network. In turn, voice traffic must accept the security risks that occur in any data network with an additional complication in that voice services are time critical

Security-Assessment.com can help provide a security strategy for implementation of VoIP. Security requirements need to be defined during the design phase of a VoIP implementation, not just tested after deployment.

An effective security strategy will assist an organisation by:

- Aligning IT security with the business needs of the organisation;
- Ensuring that security capability is in place to enable future business opportunities; and by
- Identifying security priorities so that funding and resources can be allocated where they are most required.

VoIP strategy needs to be incorporated into the organisation's security policy with defined procedures to maintain the security of the VoIP environment, including:

- Maintenance of VoIP equipment
- Administrative access to gateways
- Authentication Remote access
- Hardware IP phone controls

Voice communications remain a critical element of doing business today. Ongoing assurance and testing services are advised to maintain the integrity of the VoIP solution.

Some of the key elements that need to be addressed for securing VoIP on the network are:

- Network segmentation (data, voice and management networks)
- Network monitoring
- Business continuity and Redundancy
- Voice and email integration
- Scalability of the design
- IP phone management
- Patch management
- Incident response

Without the correct controls in place, VoIP networks are potentially open to the following attacks:

- Traffic capture attacks
- Bootp attacks
- Phone-based vulnerabilities
- Management interface attacks
- Denial of service has a whole new meaning when targeting VoIP.

Possible consequences of VoIP attacks include:

- Listening or recording phone calls
- Injecting content into phone calls
- Spoofing caller ID
- Crashing phones
- Denying phone service
- VoIP Spamming

Security-Assessment.com is able to provide strategy and policy development, including security testing and assurance of your VoIP deployment.

Security-Assessment.com offers a number of Complementary Security Services. These include:

- Threat and Risk Management Analysis;
- Security Assurance Services;
- ISO 17799 Compliance Measurement;
- Security Architecture Review and Design;
- Network Intrusion Testing; and
- System Forensic and Employee Investigation.

Contact us today on this service or any of our other service offerings:

Web [www.security-assessment.com](http://www.security-assessment.com)

Email [info@security-assessment.com](mailto:info@security-assessment.com)

Phone NZ +64 9 302 5093

Phone AUS +61 2 9570 2439

**Most advanced industry solutions**

**Highly specialised service capability**

**Enterprise class security management**

**Going beyond the audit process to provide practical solutions to real issues**

**Address environmental change in your business**

**Be proactive in managing security issues.**

