



News Channels

- [HOME](#)
- [IT Channel News](#)
- [Auto ID & RFID](#)
- [Exhibitions & Events](#)
- [Print & Label](#)
- [Data Storage](#)
- [Networking & Security](#)
- [Point Of Sale](#)
- [Document Management](#)
- [Mobile Computers](#)
- [VIDEO](#)
- [White Papers & Reports](#)



Over 300 product brochures available to order on-line

[CLICK HERE NOW!](#)

Magazine

- [Home](#)
- [Editor](#)
- [Subscribe](#)
- [Media Kit](#)
- [Mission](#)
- [Advertise](#)
- [Feedback](#)



RSS

[Advanced Syndication System.](#)

Choose all or any news channels to display on your web site.

It's good to talk - brushing off the VoIP security scare

[EMAIL ARTICLE](#) [PRINT ARTICLE](#)

With news that the Council of Europe has opted for a switch to VoIP, it seems that the technology is finally beginning to win over admirers in the corridors of power. However, fears over security are still preventing many organisations from taking the plunge.

From now on, all communications from the 4,000 seats in the Council of Europe's offices in Strasbourg will be routed through IP. The announcement represented a huge milestone for VoIP and proves that IP-based technology is being taken seriously at the very highest levels.

The Council of Europe is reportedly already using exchanges compatible with VoIP and 3,500 digital high-end lines. The core of the network has been changed and the new software platform put in place.

However, while it is clear that VoIP's destiny is no longer limited to the confines of the home office, many organisations remain cynical or are simply reluctant to implement the technology in the short-term due to concerns over potential complications in adding to an already overburdened network. Meanwhile, the technology pages are dominated with talk of the converged network. In the light of new legislation, security will be at the top of IT Directors' list of priorities when they are looking to the possible adoption of new technology by the organisation. It makes sense that as the number of ports on the network increases, so the potential for security breaches will further intensify. But this need not present a mental barrier in embracing change. If the technology offers the possibility of improved efficiency or a greater value for the tax-payer, organisations must overcome the hype cycle that results from the sentiments of a press that has traditionally thrived on scare stories.

So how can the converged network be made secure? VoIP has taken the networking industry to a stage where the fundamental approach to networking design and architecture must be updated. Security, in the broad sense of the term, sets the expectation of predictability in a system. When considering how to deliver a converged network to support VoIP along with the rest of the business applications in use, a logical approach to the functions of that network can be used to define its capabilities.

While the basic 'simple, dumb, fast' network designs of the past worked well enough for non-real-time data such as e-mail and Web traffic, ever-increasing virus and worm threats, along with the introduction of real-time applications such as VoIP to a network, mean the new model must be about a 'fast, smart, and efficient' system.

The main element of a secure converged network is the ability to control access. Most networks today have no idea who or what is connecting to them, what should or should not be done over them, and they are woefully

lacking in the ability to understand good from bad uses of the infrastructure.

The three critical components of an effective access control capability for a converged network are authentication of devices attached to the network, authorisation of the attached devices, and the policy association that is required once these former two objectives have been successfully achieved.

Policy association ensures the dynamic mapping of the correct services, privileges and access to the attached device. If a system can recognise an IP phone by authentication, but cannot dynamically associate the correct security and quality of service functions to that device, then the ability to deliver a predictable secure network will not be realised.

Another critical element of any secure converged network should be the incorporation of a dynamic response architecture. This is defined as a mechanism in which, when something unpredictable occurs in the network that can affect the reliability or integrity of the converged systems, the network can identify the threat, locate its point of origin and dynamically isolate, remove or control the threat in real time. Doing so prevents a broad, adverse impact on the system.

The recent adoption of VoIP by the Council of Europe is a promising development. It proves that the public sector is taking those tentative but all-important first steps. It is now clear that the last significant gating element threatening to delay the popular deployment of VoIP is the perception that the network is simply not ready to support voice and other applications without compromising the security and predictability of any of the shared applications.

By adopting a model of networking with security-centric thinking and by focusing on access control, proactive protection and dynamic response capabilities, it is possible to support voice on a converged network, but at the same time building a foundation equally applicable to almost any future application or service added to that system. VoIP could well prove to be the beginning and not the end in new generation technology for the public sector. Organisations should plan for the converged network, and VoIP is only one - albeit exciting - possibility in modernising and improving efficiency in working practices. Others will appear, and resellers are in a strong position to equip organisations to embrace these without fear when the time comes around.

Dean Jones is UK Channel Manager at Enterasys Networks. Enterasys Networks is the Secure Networks Company, providing enterprise customers with innovative network infrastructure products, services and solutions that deliver the security, productivity and adaptability benefits required by Global 2000 organizations. For more information on Enterasys Secure Networks and the company's products, including multilayer switches, core routers, WAN routers, wireless LANs, network management, and intrusion defence systems.



[Click to Review](#)

Related Articles :
None

Top Brochure Requests

[NetIntelligence brochures](#)

[Datalogic Range of Brochures](#)

 **Search Articles**



[More Brochures>>](#)

Sponsored Links

Datalogic

Manufacturer of CCD- and laser-based bar code readers and portable data collection terminals.

Hand Held Products

Hand Held Products is a worldwide leading manufacturer of data collection and management solutions for in-premise, mobile, and transaction processing applications.