

# Enterprise security

## So important yet so often ignored

**Ask a group of IT managers or CIOs about their key concerns, and you can bet that security will be right up there and probably the single biggest issue. Research by analysts Meta Group suggests that around 4% of total IT spending is on security, and that this will rise to 5 to 8% by 2006.**

What is meant by security is a moving and complex discussion. Security experts claim that it takes up to 20 years to resolve all the security issues for a new technology. Little wonder then, that CIOs view new IT and telecoms technologies from Wireless LANs to IP telephony to grid computing as fraught with security problems.

New security terms and challenges have also recently entered the IT world. These include the endemic fear of the online banking community, phishing. This is when a fraudulent email, pretending to be from a trusted provider, tricks users into giving away passwords and other important information. Another term to strike fear into the IT department is Denial of Service. This is when a router, network or Web site is flooded with more traffic than it can handle, causing it to crash. In what sounds like a science fiction movie, the perpetrators often use trojan horses to infect broadband connected PCs, which then turn into

**Part of the challenge is getting control of all the different and complex aspects of enterprise security.**

what is described as a "zombie army." The truth is far more serious, with analysts Forrester Research estimating that a denial of service attack can typically cost a company \$100,000 an hour. In reality, the cost could be far higher.

Security has also become more important due to increased regulatory and compliance pressures, particularly in industries such as finance and health care. This trend is likely to continue and increase in the Asian markets.

### What should an enterprise do?

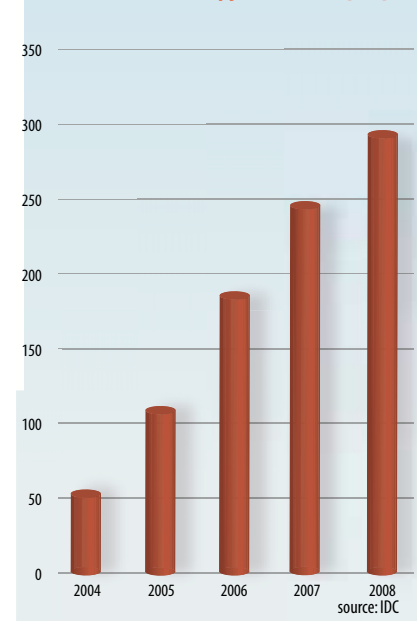
Part of the challenge is getting control of all the different and complex aspects of enterprise security. One of the most frustrating aspects of security is that it is a "moving target" rather than a finite problem; that is, you can never really be 100% in control of security issues. Analysts at Gartner Group believe that four security processes are critical: network access control, intrusion prevention, identity and access management and vulnerability management.

One of the weaknesses of many organizations is that they have purchased individual point products to handle the different security challenges. This has led to soaring demand for individual products such as anti-spyware software.

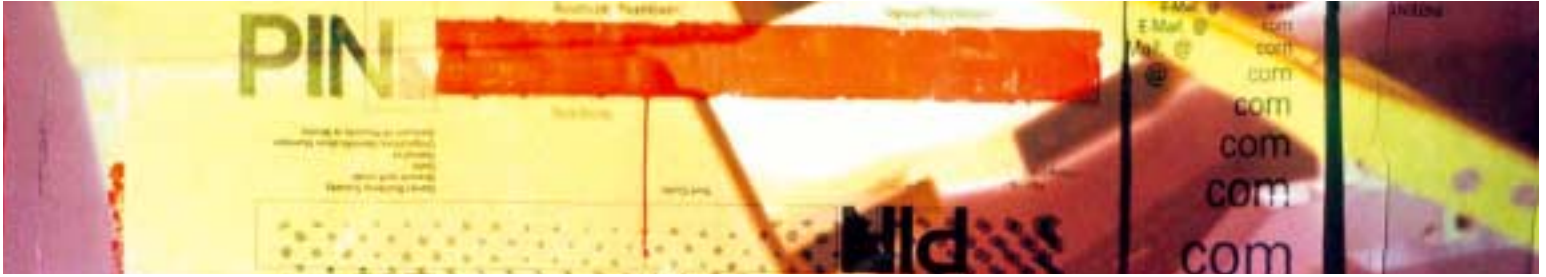
It is far more sensible for enterprises to take a more integrated approach to security. This should involve both internal and external parties. Internally, security should not be just the focus of the IT department or even a security department, but a factor for all business groups. Externally, enterprises should look to work with key partners rather than buying lots of different security products.

One recent move that will help to consolidate the security market has come from Microsoft. It has stated that it will provide anti-spyware functionality free to licensed Windows users for personal and home use by the end of 2006, although enterprises will have to pay a fee. By the same timeframe, it will offer a consumer anti-virus service. It appears likely that Microsoft will develop a full security suite for enterprises within the next three to four years.

Worldwide anti-spyware sales (\$m)



Another solution for enterprises is a managed security specialist. There are natural concerns about outsourcing something as critical as enterprise security, but then security requires great expertise, so it makes sense to look for a partner who has that level of skill.



**Enterprise mobility – finally coming of age**

Mobile networks are getting faster, from the GPRS networks and third generation (3G) licenses being prepared in China to the so-called 3.5G networks being built up in Japan and South Korea. Devices are getting smarter, from the mobile wallet of the DoCoMo FeliCa handsets to sophisticated new enterprise handsets. There has also been an increased focus on enabling enterprises to mobilize applications, not just from the mobile vendors but from traditional IT vendors such as IBM, Oracle and HP.

**Drivers for enterprise**

According to research from analysts Gartner Group among enterprises in Asia-Pacific, the biggest drivers for mobile and wireless solutions deployments are improved speed, timing and access of information. Other benefits were perceived as competitive advantage and differentiation, and reduced costs resulting from wireless deployments.

**The biggest obstacle to enterprises using mobile solutions is always security.**

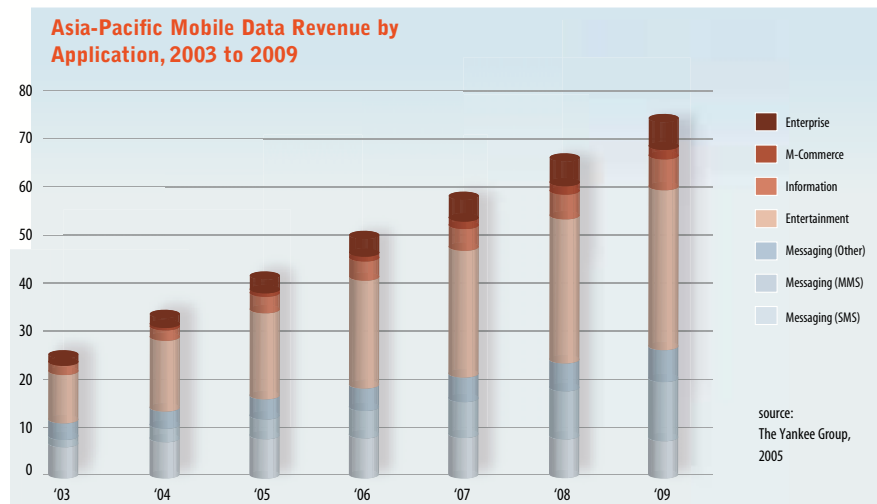
Although it is clearly a business benefit to get information more quickly, it is difficult to quantify this benefit. This has been one of the challenges for the mobile industry in selling to enterprises. An easier sell has been when clear cost savings or efficiencies can be demonstrated. This has been particularly true in markets such as field sales and transportation, where administration posts can be reduced as information is processed by mobile workers, often in real-time rather than at the end of the day. Although again it is often difficult to quantify, such early adopters have often been able to provide a much enhanced customer service experience. For example, letting customers know instantly whether something is in stock and available for purchase. The higher speeds and greater reliability of new mobile networks are essential for such projects.

Mobile solutions have also become a lot more interesting for many enterprises with the explosion of wireless hotspots, offering up to 11 Mbit/s – many times faster than 3G. A new technology, WiMax, offers far greater speeds, up to 70 Mbit/s, over a far greater distance, up to 50 kilometers, although it is unlikely to be commercially available for several years. A key issue for enterprises will be integrating these different technologies so employees can use the most appropriate technology at different times.

international roaming and large data downloads. A further obstacle in markets such as India and China has been the mobile coverage outside the larger towns and cities.

**The winners**

The mobile operators would like to manage services for enterprises but often users would prefer to get mobile solutions from their traditional suppliers such as systems integrators and IT vendors. However, the mobile operators will always benefit



**Key obstacles**

The biggest obstacle to enterprises using mobile solutions is always security. Will a mobile user prove to be the “weakest link” in enterprise security? Surprisingly little vendor activity has been undertaken in this area, and startups are often the leading providers.

The other key objection is the return on investment. Given the difficulty in quantifying mobile benefits, how do you measure the results of your investment? While IT spending has often been closely managed and budgeted, mobile spending is often spread between many business units. Each business unit may also account and measure mobile spending in different ways. Mobile pricing is often considered too high and difficult to understand for enterprises. This is particularly true in areas such as

from the increased traffic on their networks and much of their data revenue will come from other areas such as entertainment.

The challenge for other vendors is whether the IT manager wants to use a company that understands mobile and wireless solutions, or a company that understands IT solutions? Ideally, of course, they want both, and this will make it very hard for those vendors who either are 100% focused on the mobile market, or are IT vendors struggling to work within the limitations and quirks of the mobile environment. It will help large vendors such as Ericsson and Nokia, who do understand both the IT and mobile environment. ■

Written by Steve Wallace  
Designed by Step Design Consultants