

Point-to-Point

Gartner

28 November 2001
Vol. XVI, No. 11

ENS, ENSC, ENSE and LAN Services

Management Update: Gartner's Information Security Hype Cycle Helps Reduce Risks

Many CEOs, CIOs and other enterprise executives are becoming increasingly worried about how their enterprises can address the growing threat of information security risks. To help those executives with their planning, Gartner discusses its Information Security Hype Cycle, covers important 12 emerging technologies and provides recommendations. Investing in an overhyped technology too early can result in a complete waste of enterprise security funds. Enterprises should focus on their assessment of business needs and threats to prioritize security needs.

When Should a New Technology Be Deployed?

Each new wave of technology disrupts existing security measures and introduces its own new vulnerabilities. Overlaying that local source of
(continued on page 2)

Management Update: Use Videoconferencing to Cut Travel, Reduce Costs

With air travel increasing in difficulty and expense, many enterprise executives are looking for solutions such as low-cost videoconferencing that can keep workers at their desks. To help those executives with their planning, Gartner discusses how low-cost systems can help, but infrastructure is a barrier to quality.

Two Videoconferencing Categories

Enterprises can save money by cutting back on travel and substituting videoconferences for some face-to-face meetings. The savings come both in actual travel costs and in the costs of having employees out of action during a trip. However, videoconferencing should be implemented with care. The two general categories, conference room systems and desktop systems, have different benefits and drawbacks, but both impose costs and complexities beyond their initial installation.
(continued on page 8)

In This Issue...

1

**Management Update:
Gartner's Information Security
Hype Cycle Helps Reduce Risks**
Gartner discusses its Information Security Hype Cycle, covers important 12 emerging technologies and provides recommendations that enterprises can follow.

1

**Management Update:
Use Videoconferencing
to Cut Travel, Reduce Costs**
With air travel increasing in difficulty and expense, many enterprise executives are looking for solutions such as low-cost videoconferencing that can keep workers at their desks.

10

**Management Update:
Audioconferencing Can Yield
Cost Savings, Improved Service**
Audioconferencing solutions on software platforms with Web-based self-service have the potential to reduce enterprise costs while increasing service.

13

**Management Update: Time to
Tighten Security Measures for
Malicious Telephone Calls**
Many enterprises executives are quite concerned about security issues, as well as the associated privacy issues associated with heightened security measures. Enterprises have many tools with which to track and stop malicious calls.

14

Cross Talk

Management Update: Gartner's Information Security Hype Cycle Helps Reduce Risks (continued from page 1)

chaos, each new technology in the security, privacy and risk management domain follows the hype cycle. This additional layer of misperception amplifies the technology's disruptive impact.

Determining when to adopt an emerging technology is a critical decision. If an enterprise launches its efforts too soon, it will suffer unnecessarily through the painful and expensive lessons associated with deploying an immature technology. If it delays action for too long, it runs the even-greater risk of being left behind by competitors that have succeeded in making the technology work to their advantage, or runs the risk of leaving the enterprise open to vulnerabilities the new technology addresses.

The decision can be eased by understanding the hype cycle model of emerging technologies, introduced by Gartner in 1995. The hype cycle highlights the pattern of overexpectation, disillusionment, and eventual maturity and productivity that accompanies most emerging technologies

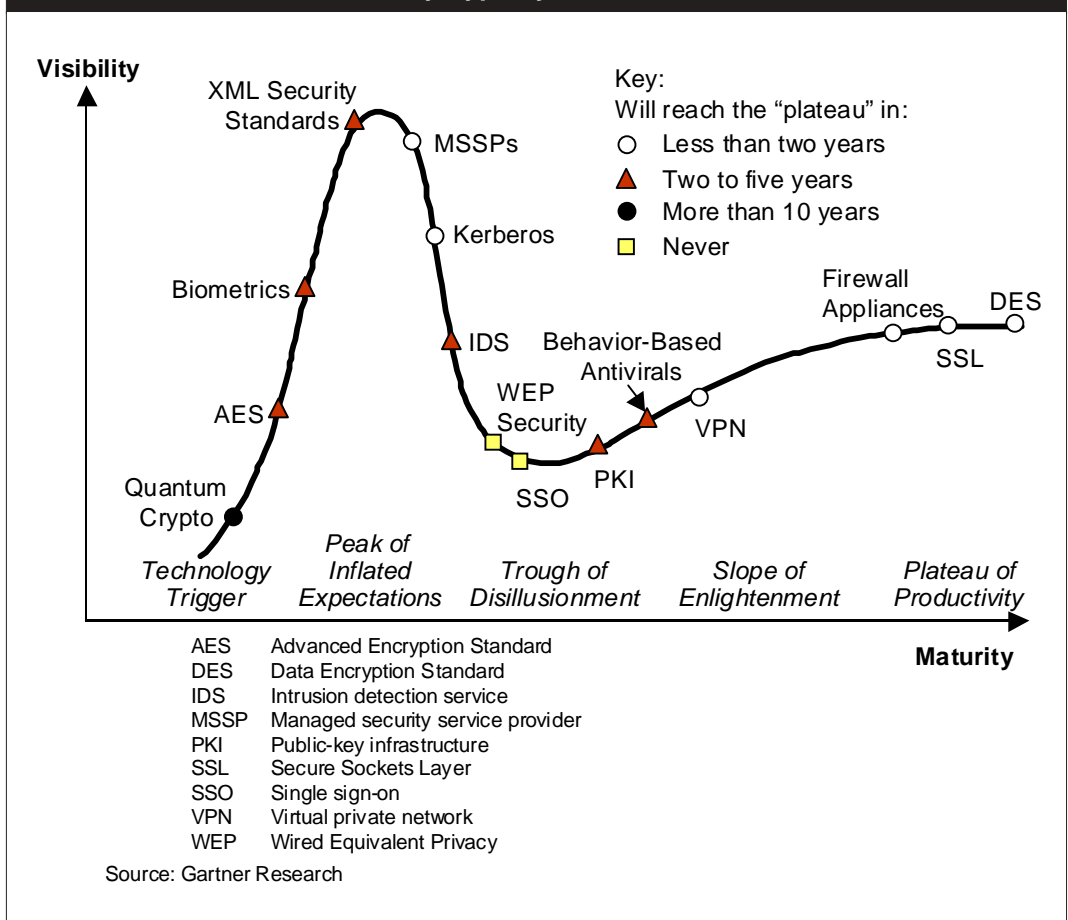
(see the sidebar, "The Five Phases of the Gartner Hype Cycle").

Adoption Guidelines

Generally, the more important a technology is to an enterprise's competitive advantage, the more important it is that a "first-mover" advantage be pursued. However, technologies that will bring only incremental, tactical or operational value should be adopted later in the

cycle, as they mature and stabilize, and as a clear return on investment (ROI) can be identified. However, information security cannot be looked upon from an ROI or competitive advantage perspective. Many security technologies are defensive in nature. Enterprises should evaluate the changing information security landscape in the context of their specific defensive requirements and avoid letting the vicissitudes of the hype cycle and the relative

Figure 1
The Gartner Information Security Hype Cycle



Entire contents © 2001 Gartner, Inc. All rights reserved. Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice. Additional subscriptions may be ordered for an annual fee (\$500 in the United States for 12 issues per year; higher pricing may apply elsewhere). Multiple reprint prices are available on request; contact Gartner at +1-203-316-1111. Comments can be e-mailed to: inside@gartner.com.

The Five Phases of the Gartner Hype Cycle

The five Gartner Hype Cycle phases are:

- **Technology Trigger.** A breakthrough, invention, discovery, public demonstration, product launch or other event generates significant press and industry interest.
- **Peak of Inflated Expectations.** During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the technology is pushed to its limits. The enterprises that make money during this phase are generally conference organizers, magazine publishers and consultants.
- **Trough of Disillusionment.** Because the technology does not live up to its inflated expectations, it rapidly becomes unfashionable, and the press abandons the topic or touts its failure to meet expectations.
- **Slope of Enlightenment.** Focused experimentation and solid hard work by an increasingly diverse range of organizations leads to a true understanding of the technology's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools become available to ease the development process and application integration.
- **Plateau of Productivity.** The real-world benefits of the technology are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. The final height of the plateau varies according to whether the technology is broadly applicable or benefits only niche markets.

popularity of any particular security solution dictate plans.

The Information Security Hype Cycle (see Figure 1) works to identify where in its life cycle each critical technology component can be placed. The chart also shows when Gartner expects the technology to reach the plateau of productivity representing general acceptance in the marketplace.

Quantum Cryptography

Without knowing the key, encrypted files are broken by brute force attacks — by trying every number in the keyspace until the right combination is found. It has been speculated that advances in factoring, or the ability to detect repetitions in a vast amount of ciphertext as clues to the prime numbers used to encrypt, may lead to easier cryptanalysis. (Keyspace is the name given to the

range of possible values for a cryptographic key.) Most mathematicians familiar with the subject, however, are not optimistic.

Advances in the esoteric area of quantum computing, with machines operating in the petaflops (one quadrillion, or 10 to the 15th power, floating point operations per second) and exaflops (one quintillion, or 10 to the 18th power, floating point operations per second) range, and based on the performance of individual atoms, may prove more fruitful.

Work being done by the National Security Agency, the Defense Advanced Research Projects Agency, academic institutions, IBM, Hewlett-Packard and others has already demonstrated the potential of these machines to search keyspace very rapidly to decipher strongly encrypted messages. Once developed, quantum cryptanalysis machine availability will be limited for a period of time. As the technology proliferates and becomes less expensive, quantum encryption itself will also become available — but only to those who can afford it.

Recommendation: Enterprises need not worry that quantum computers will be regularly used to break encrypted messages before 2006. Even then (as now), only single messages will be broken, and only messages protected with public-key approaches will be vulnerable. Strong encryption as defined today is sufficient to protect commercial

Management Update: Gartner's Information Security Hype Cycle Helps Reduce Risks (continued)

secrets. Quantum cryptanalysis will be first applied to intelligence and national defense activities, and thus will be of initial importance to relevant agencies.

Biometric Identification and Authentication

It is difficult to cost-justify the "something you are" of biometrics as a means of identification and authentication for access control in enterprise settings. Biometric vendors are very small and unprofitable. Despite pilots, testing and usage in physical access control systems for data centers, biometrics have remained expensive, with unacceptable error rates and human acceptance problems.

While fingerprint readers, the most-probable approach for enterprise use, are dropping in price and can be integrated with keyboards, laptops, personal digital assistants (PDAs) and cell phones, some systems can be fooled by rubber molds; the features that check for "liveness" add considerable cost. Nevertheless, as the price continues to drop during the next two to five years, integration will follow.

Biometrics overcome the risk of the person seeking access not being authorized due to compromised passwords or shared tokens. However, Gartner believes any wide-scale use of biometrics for access control will be followed by a privacy backlash in most countries. Current large-scale public deployments of

facial scanning systems in airports, sports venues and other public spaces for safety and law enforcement purposes have different characteristics than enterprise systems, but may be indicative of technology directions and public acceptance of biometrics.

Recommendation: Biometrics are in the advanced technology evaluation stage, but enterprises can continue to test a variety of devices for niche applications, such as physical security and for protecting highly sensitive systems, including automated teller machines. Facial and iris recognition systems (which have the highest accuracy) offer some appeal, especially because the cameras can also be used for video applications.

XML Security Standards

XML has rapidly gained acceptance because of its text-based format and ease of use, but the information is completely "in the clear," and therefore can be read by anyone with access to the document. In addition, portions of the XML document or electronic form might need to be protected by one party and altered by another, thereby invalidating the security if the entire document was protected.

Under development in products and standards are several XML security-related standards, such as an XML Digital Signature recommendation that defines the processing rules and syntax for XML digital signatures. This standard

would allow the scope of the signature to be matched to the hierarchical structure of XML documents. Without a structured signature scope, a change by one party to one portion of the document would invalidate the entire document.

Furthermore, an OASIS (Organization for the Advancement of Structured Information Standards) working group plans to develop a XML security standard called the Security Assertion Markup Language Standard (SAML) that will address user authentication and authorization. Its main goal will be to provide interoperability between security products in the extranet asset management space and Web content management software. One problem is the proliferation of sometimes-overlapping approaches, causing market confusion. In addition, Microsoft has recently provided a high-level overview of its approach to XML security as part of its Global XML Architecture. While details are still sketchy, the company's action will negatively impact SAML in particular.

Recommendation: When possible, enterprises should select security solutions that are compliant with open standards rather than proprietary solutions. To meet interim needs, enterprises can use proprietary solutions or incomplete standards and achieve interoperability through bilateral negotiations.

Managed Security Service Providers

Just reaching the peak of inflated expectations are managed security service providers (MSSPs).

Outsourcing security, first with firewalls, then intrusion detection service and other services, is increasingly making sense to enterprises for a variety of reasons. The first round of MSSP market entrants, however, are now facing the realities of not being accepted beyond their first customers because of their relatively small size. In addition, they have personnel retention issues in not being able to offer staffers much in the way of career advancement.

The next phase will be a series of mergers and acquisitions while larger security firms such as Symantec and consultancies start offering credible managed security services. Gartner believes that the use of MSSPs will rapidly reach the plateau of productivity after the industry shakeout settles down.

Recommendation: Enterprises lacking security staff, or having three or more intrusion detection service sensors, should evaluate MSSPs to help them provide due care levels of security.

Kerberos

This authorization routine, initially introduced as part of the Distributed Computing Architecture, was considered passe, but has now returned to some degree of impor-

tance. Built into Windows 2000 and XP, Kerberos has been around since the mid-1980s, but never escaped niche use.

Microsoft's inclusion of Kerberos in Windows 2000 and Windows XP, and the recent announcement that its Passport authentication service would be based on Kerberos by 2003, means that for business-to-consumer transactions, Kerberos will be increasingly important. Microsoft's goal is to replace Web browser to Web server authentication interactions with desktop operating system to server operating system interactions via Kerberos. Because Kerberos supports many optional and application-specific fields, there will be many interoperability problems in the future if Microsoft succumbs to the temptation to embrace and extend yet another standard.

Recommendation: Because Microsoft operating systems dominate the desktop and will be an increasingly strong player in the PDA space, most user-facing applications will need to interface with Kerberos during the next three years. Enterprises should require their extranet asset management and portal vendors to detail plans for integrating Kerberos authentication and access management.

DES and AES

Still early in the hype cycle is the new Advanced Encryption Standard (AES) selected by the U.S. Department of Commerce (and specifically

the National Institute of Standards and Technology, or NIST) to protect electronic information. AES will officially replace the government-endorsed Data Encryption Standard (DES), adopted in 1977. AES will eventually become the preferred symmetric data encryption standard for most private enterprises.

DES has become susceptible to brute-force attacks by networks of code-cracking computers. Accordingly, DES is at the end of its life cycle. It is estimated that code-cracking computers would have to work 149 trillion years to decipher an AES encryption key. Under the rules of NIST's selection, the algorithm carries no royalties, although software implemented using cryptographic toolkits may require per-seat or negotiated fees. Although the NIST says that other considered algorithms such as Mars, RC6, Serpent or Twofish might be more efficient than AES in some applications or implementations, Gartner expects AES to find the most usage because of its endorsement as the "standard."

Recommendation: It will take some time before most security products in the field are updated to include AES. AES will likely not replace more than 30 percent of DES operations before 2004. Enterprises using DES should plan on migrating to AES as soon as it is feasible. However, those using the stronger 3DES standard should wait until system upgrades permit a low-cost AES implementation, unless they are experiencing

Management Update: Gartner's Information Security Hype Cycle Helps Reduce Risks (continued)

unacceptable system sluggishness because of the performance characteristics of 3DES.

Wireless Security

The wireless world faces continuing problems in developing secure solutions, with the Wireless Application Protocol initiatives facing slow advancement due to usability and performance problems in the cellular Internet space. Gartner believes that Wireless Transport Layer Security (WTLS) will prove sufficient for the next few years in the slowly growing mobile commerce world. As early as 1999, Gartner pointed out several weaknesses in the Wired Equivalent Privacy (WEP) security function in the 802.11b WLAN specifications. Enough additional weaknesses were found in WEP in 2001 to require a nearly complete redevelopment of WLAN security specifications. Even if the future (2002) 802.11i security specification retains the name WEP, the original concept of WEP will never reach the plateau of productivity.

Recommendation: Enterprises planning mobile applications where security is required should develop applications based on WTLS in the short term, while looking to the 802.11i standards for second-, and possibly third-generation implementation of wireless LANs.

Single Sign-On

The products representing the promise of single sign-on are firmly

in the trough of disillusionment because they offer limited application integration and limited cross-platform support. While arguably a user convenience rather than a security solution, single sign-on providers will face further uncertainty as a result of Microsoft's introduction of Passport and competing products from the Liberty Alliance and America Online. These offerings are primarily intended to allow consumers to sign on to, for example, an online brokerage, and then surf to another site without needing to identify and authenticate a second time. Nevertheless, Passport and others will impact corporate single sign-on attempts. Gartner believes maturity of single sign-on products as currently offered will prove illusive for 10 years or more, because the problems of heterogeneous support will remain.

Recommendation: Reduced sign-on is possible for a limited number of applications on homogenous platforms; enterprises should concentrate single sign-on development where the user experience must be improved, or where users are now required to have 10 or more regularly used user ID and password pairs. Password management and synchronization systems should be used to control the costs of user password resets and the proliferation of account details that must be remembered.

Public-Key Infrastructures

Applications requiring centrally public-key infrastructure (PKI)

continue to move slowly. For example, there is little uptake of the S/MIME standard for secure e-mail. Other applications that could benefit from PKI can often manage the digital certificates within the application. Gartner has discussed the PKI hype cycle in previous research. While centrally managed PKI will have a place, most implementations of PKI will change from this idealized vision to become invisibly integrated with reliant applications.

Recommendations: Enterprises that have made a substantial investment in centralized PKI should maintain their investments with a view toward demonstrating value within a two- to three-year time horizon, as infrastructure investments may take some time to show benefits. Enterprises should focus on their need to manage cryptographic keys as part of specific applications rather than look to PKI as "pure technology" with applications to follow.

Behavior-Based Antiviral

Signature-based antiviral protection is broadly deployed and enjoys a position in the plateau of productivity, but needs to be replaced by behavior-based solutions at the desktop. Signature antivirals require frequent updates to the desktop, which is problematic when users are not regularly connected to the corporate network for pushed updating. In addition, viruses rapidly mutate so that protection against one does not protect against

another, but similar, variant. The value of signature-based antivirals is decreasing. Accordingly, products that watch for and respond to the behavior characteristics of viruses (replication, or attempting to access the address book, for example) will become more effective in the 2005 time frame. This capability will become more necessary as Web services and the increased potential for malicious software sweep the enterprise.

Recommendations: Enterprises should evaluate their current and projected adoption of active content and XML-based applications and Web services as a barometer for determining when to transition away from desktop signature-based antivirus solutions. Windows 2000/XP rollouts can also be used as transition points for moving away from these solutions. Gartner recommends that enterprises have some behavior-based malicious-code detection methods in place by 2003. Signature-based antivirus solutions on servers (internal e-mail or boundary firewall) should be used as an interim measure through 2005.

VPN

Virtual private network (VPN) technology using a variety of protocols has moved up the slope of enlightenment, driven by the clear cost savings offered over alternatives such as direct leased lines and value-added networks. Although standards wars and problematic issues remain (over the IPSec

protocol specifically), whole industries, such as the automotive industry, have moved to VPNs as the basis of extranets for e-business and other activity. VPNs are now in the plateau of productivity.

Recommendations: Before deploying an IPSec-based VPN, enterprises should analyze the applications that will be carried over it. If all applications are browser- or HTTP-based, a Secure Sockets Layer-based solution will be less expensive and more secure than an IPSec tunnel.

Firewall Appliances

Enterprise firewalls have matured, become ubiquitous and now dominate the firewall market. Appliances provide greater performance and higher security at a reduced cost of ownership. Recently introduced “in-the-cloud” firewalls provide a means for less-expensive and faster managed firewall solutions, whether managed internally or by an external MSSP. Gartner believes in-the-cloud firewalls will begin to have market impact in 2H03.

Recommendations: Enterprises replacing or expanding firewall architectures should abandon software-based firewalls in favor of firewall appliances. Enterprises utilizing Internet Data Center or Internet service provider hosting facilities should look to in-the-cloud firewall services if providers offer them at a cost reduction of 20 percent or more over individually managed firewalls.

Bottom Line

- Investing in an overhyped technology too early can result in a complete waste of enterprise security funds.
- Enterprises should focus on their assessment of business needs and threats to prioritize security needs.
- This analysis should be combined with the Gartner Information Security Hype Cycle to deflate the hype spread by security product and service vendors.

Written by Edward Younker,
Research Products
Analytical sources: John Pescatore
and Vic Wheatman,
Information Security Strategies

For related articles published in Point-to-Point, see:

- “Management Update: Mobile and Wireless Security — Worst and Best Practices,” 26 October 2001
- “CIO Alert: Plan for Increased Internet Security After Terrorist Attacks,” 26 October 2001
- “CIO Update: VPN Security and Placement,” 28 September 2001
- “Management Update: The Gartner 2001 Hype Cycle — Emerging Trends and Technologies,” 31 August 2001

Management Update: Use Videoconferencing to Cut Travel, Reduce Costs (continued from page 1)

- Room systems are relatively expensive (starting at approximately \$5,000) and generally work over switched circuits (generally Integrated Services Digital Network, or ISDN), which ensure high quality but impose ongoing costs.
- Desktop systems are relatively inexpensive (approximately \$500) and work through the enterprise network. However, the heavy traffic they generate can affect the infrastructure significantly, and network upgrades may be needed to make the experience better than annoying. Beyond their own performance, moreover, looms a risk to the enterprise at large: since its bandwidth demand scales with the number of users, uncontrolled conferencing can quickly overload a network and hurt the performance of other applications and users.

For these reasons, Gartner recommends that enterprises stick with ISDN room systems through 2003. However, room systems can be run in network mode as well, so the equipment need not be replaced to realize ongoing savings.

Entry Level: The Webcam

The lowest level of conferencing is the “webcam,” a small video camera that mounts on a monitor or laptop screen. Logitech, 3Com and other vendors sell them for less than \$100. They generally use Microsoft NetMeeting as a user interface, although dedicated client applica-

tions are available from vendors such as Earthcam, Paltalk, Dwyco, iSpeed, iVisit and Firetalk. This webcam approach is the least successful because it is a software-only solution that relies on the desktop processor to do all the work — and even the most powerful desktop will not perform as well as the specialized signal-processing hardware in a dedicated appliance.

Moreover, some products do not conform to the H.323 videoconferencing protocol, and may have difficulty connecting with other types of equipment. On balance, despite their low cost, the limited performance and standardization of webcam solutions keep them from being a business-class alternative for videoconferencing.

Substituting a conventional video camera sounds attractive, but adds significant cost and complexity. Cameras with digital outputs cost as much or more than a dedicated conferencing appliance; most do not have Universal Serial Bus (USB) connectivity, so a FireWire interface must be added.

Analog cameras are less expensive, but require an encoder or capture card that would raise the price to the same level. Moreover, video cameras are not physically designed to sit on a flat surface, and must be positioned on a tripod or other accessory that is not at home on a desk. Since such an arrangement would not be dedicated but user-assembled, the user would face additional software and configuration complexity.

- **Pros:** Very low cost
- **Cons:** Low quality; dependent on user configuration and desktop capabilities; incomplete standards compliance; no multipoint capability; widespread use can overload network

Intermediate: The Video Appliance

The next step up is the video appliance, a self-contained box that integrates a higher-quality camera with dedicated compression and encoding hardware. This approach is much more successful because the dedicated hardware processes the signal much more efficiently than a desktop CPU. Moreover, the price differential is small — a few hundred dollars instead of \$50 or \$100 for a webcam.

The leading appliance is Polycom’s ViaVideo, which sells for approximately \$500 and plugs into a USB port to deliver a ready-made H.323 data stream to the desktop system. The desktop video appliance is the minimum desktop solution that Gartner recommends for business use, and in environments where network conferencing is technically feasible it constitutes an effective low-cost collaboration tool. Most will allow whiteboarding, presentation and application sharing using Microsoft NetMeeting. They all conform to the H.323 specification, so they can connect with any other H.323 device. However, they can only connect with other network-based systems, not with ISDN (H.320) systems, unless there is a

gateway at either end to connect the two protocols.

Aside from Polycom, other vendors include VCON and Zydacron, and prices range from \$400 to \$1200. USB products are more practical than those that connect through a PCI board, which are more costly and labor-intensive to install.

- **Pros:** Low cost; higher quality than webcams; packaged solution eases configuration; standards-compliant; some models can be remotely managed
- **Cons:** Lower quality than group systems; some user configuration required; separate audio connection may be needed); no multipoint capability; widespread use can overload network

Advanced: Group Systems Are Alive and Well

Group conferencing provides the highest level of quality and ease of use by a large margin, but has always been regarded as expensive and complicated to install. However, group systems are not nearly as expensive as they once were. Low-end Viewstation models from Polycom sell for less than \$5,000, plus the cost of a monitor (a regular TV monitor will do), and most room-based vendors are now making low-cost systems with similar core conferencing functions. The cost, however, is 10 times as much as that of a desktop appliance, and the common use of ISDN lines makes

group systems seem old-fashioned. The urge among videoconferencing users and vendors is to move away from costly telephone circuits and toward network conferencing, with extensive data integration so that people can see what they are working on as well as each other.

However, network conferencing is still fraught with glitches and inefficiencies, only some of which can be corrected by adding more bandwidth. Most are created by packet losses, collisions and delays in the routers that can only be fixed in the lower levels of the network. Except for automated teller machine networks, which can create virtual circuits, most networks do not ensure that a stream of packets is received in the same order in which it was sent. Moreover, disruptions in packet sequence and timing lead to lost pixels, dropped frames and loss of sync between sound and picture that can make the conferencing experience not just unsatisfying but actively unpleasant. As a result, Gartner recommends that through 2003, mission-critical meetings, especially those involving senior executives with a low tolerance for technical glitches, be conducted over a minimum of three ISDN pairs (384 Kbps) to ensure reliable quality.

Even the best room system is less expensive than travel, however. A transcontinental or transatlantic trip for a single executive for a one-day meeting can cost \$2,000 to \$3,000; a saving of 10 such trips can pay for a robust conferencing installation. Moreover, ongoing costs will decline

and return on investment will increase over time as networks are upgraded and the quality differential declines. All room systems can use either the network or ISDN protocol, and quality-of-service technologies now being developed and deployed will likely increase network performance enough to make it a lower-cost alternative of comparable quality by the end of 2003 — well within the lifetime of the equipment.

- **Pros:** High quality; multipoint capability; ease of use; IP or ISDN operation; many options and accessories available; can accommodate large groups; fully standards-based
- **Cons:** High cost; “public” facility requires IS or departmental administration, scheduling and oversight; ISDN use generates ongoing expenses

Bottom Line

- Enterprises can save money with videoconferencing by reducing travel, but neither the initial investment nor the ongoing cost is trivial.
- From tier to tier of videoconferencing formats, the tradeoff is between complexity and cost on the one hand, and reliability and quality on the other.
- Network-based conferencing will provide a reliably satisfying experience by the end of 2003, but networks will have to be upgraded to make use of it.

Management Update: Use Videoconferencing to Cut Travel, Reduce Costs (continued)

- The consumer “webcam” is suitable only for personal use, for ad hoc collaboration in a robust environment or where quality is not an issue.
- Desktop video appliances can deliver acceptable performance if network infrastructures are optimized.
 - They may be suitable for workgroup collaboration where integration of document content is important.
 - When desktop appliances are

deployed, administrative controls will be needed to prevent network overload if concurrent use becomes excessive.

- Room-based, circuit-switched conferencing provides the best quality, reliability and ease of use, but with higher initial cost and ongoing line charges.
 - It is recommended for mission-critical uses or when senior executives are involved.
 - Systems can be installed with

ISDN lines and migrated to network protocols when the infrastructure is sufficiently robust.

Written by Edward Younker,
Research Products
Analytical source: Lou Latham,
New Media Technologies

For related articles published in Point-to-Point, see:

- “*CIO Update: Buy Smarter and Better Instead of Less When Networking Budget Cuts Hit,*” 25 May 2001

Management Update: Audioconferencing Can Yield Cost Savings, Improved Service

Many CIOs and other enterprise executives are scrambling, in these difficult economic times, to find ways to save money. To help those executives with their planning, Gartner discusses how audioconferencing solutions on software platforms with Web-based self-service have the potential to reduce enterprise costs while increasing service. To achieve savings, management tools, reports and defined procedures are critical.

Increasing Use of Audioconferencing

Conference calls are ubiquitous in today’s enterprises. The increasing use of conference calls is driven by many factors:

- Geographically dispersed organizations
- Widespread use of teams
- The increased use of wireless phones by mobile workers
- Severe restrictions in travel

Consequently, enterprises should re-evaluate their approach to audioconferencing. Bringing the conferencing facility in-house enables enterprises to obtain up to 40 percent savings (0.6 probability), or at a minimum, will better position them for more-competitive bids from outsourcers.

Before committing entirely to an all-in-house solution, enterprises working with customers or offering services via audioconferencing must

balance savings against possible lower response times, fewer support services and limited disaster recovery procedures. In such cases, a combined in-house and outsourced solution may better match needs. However, in that case, service-level agreements and penalties must be defined to ensure the availability of service provider resources.

Evaluate the Savings

Enterprises must evaluate the hard savings (see the sidebar, “Hard Savings”) as well as the soft savings. The savings should then be considered in terms of the operating expenses (see the sidebar, “Operating Expenses”) and the purchase costs (see the sidebar, “System Sizing

Hard Savings

- **Average number of conferences (NC) per month.** Industry average is 0.5 per employee per month.
- **Average duration of conferences (DC).** Average scheduled time is 60 minutes, but many conferences actually last only an average of 30 minutes.
- **Average number of participants (NP).** Average is six, with a common range of four to eight.
- **NC x DC x NP = CM (conference minutes) per month.** With those average usage figures for an enterprise of 1,000 employees, $CM = 500 \times 30 \times 6 = 90,000$ conference minutes per month.

Cost model:

- At 20 cents per minute, outsourced costs would be \$18,000 per month. Note that other outsource charges are not included.
- Based on the conference minutes per month, this enterprise would need 30 ports ($90,000/3,000$).
- At \$3,500 per port, the system would cost \$105,000, and the payback period would be less than six months.

and Cost”), as well as in terms of the service risks outlined earlier.

Leading enterprise audioconference bridge vendors include:

- Latitude Communications (www.latitude.com)
- Octave Communications (www.octavecomm.com)
- Spectel (www.spectel-multilink.com)
- Voyant Technologies (www.voyanttech.com)

Soft Savings

While soft savings are often difficult to quantify, they can be significant. For instance, with an in-house solution, the telecommunications traffic charges (local and long-distance) go against the enterprise’s rate reduction. Another soft saving is the convenience of ad-hoc and always-available conferences; especially with today’s travel restrictions, and it often improves group communications and cohesion. Security on in-house systems can be directly controlled, and if needed, each caller can have his or her own ID and security code and use a secure line. Individual IDs

also simplify the departmental bill-back functions.

In the cost model that Gartner provides, many of the service provider fees are not considered as hard savings, including the cost of dynamically adding users and the cost of extending the call duration, as well as the charges for canceling or changing times of conferences. Those are functions that are handled at no charge for in-house solutions. However, although moving away from “operator-assisted” to “reservationless” and “self-service” will reduce costs, ease of use and proper training is critical if employees are to use the self-service model.

Features and Functions

Audioconferencing systems are evolving along the trajectory common to telecommunications products — they are shifting focus from hardware to software, leveraging the Internet and becoming increasingly

Operating Expenses

- **System administrator.** Full-time administrator is not needed. Minimum of one-eighth-time administrator, and a one-quarter-time position for 700 ports of bridge.
- **User support.** Varies based on level of assistance users will require and the peak period loads. Typically handled as part of the enterprise help desk and estimated as one help desk person for every 240 ports, or every 750,000 minutes of usage.
- **Conference moderator or operator.** Varies depending on whether assisted conferencing is required; someone must listen and be available to announce questioners. In most enterprises, the percent of conferences with this requirement is low (5 percent to 10 percent). These could be outsourced.
- **Service and support.** Estimated at 12 percent to 16 percent for 8x5 and 16 percent to 20 percent for 24x7.

Management Update: Audioconferencing Can Yield Cost Savings, Improved Service (continued)

System Sizing and Cost

- System administrator. Full-time administrator.
- Systems are typically priced at an average of \$2,000 to 4,000 per port.
- A good way to size port requirements is to extrapolate from current usage levels for outsourced bridges and use the estimate of one conference port for every 3,000 minutes of monthly usage. In some cases, current outsourcers can provide detailed reports about concurrent sessions, and these can be used to form an estimate. Note, however, that outsource records do not always reflect actual demand, as many users and departments are significantly more reluctant to use pay-per-usage services. Because of this, easy scaling is a critical evaluation criterion.

integrated with other applications. As that happens, the features and functions available also increase. Key functions fall into several categories.

Platform functions include:

- Scalability
- Reliability
- Uninterruptible card replacement
- Strong remote support options

Report functions can be critical, so both default and flexible exporting of data are required. When call-assistance agents are involved, the ability to integrate reports of automatic call distributor agent activity with trunk usage and with the conferencing system ports can be useful for trouble tracking.

Scheduling and user profile administration is an area in which Internet options are increasingly vital. Useful features can include scheduling via manual interface, phone (interactive voice response), Web and automated e-mail form. The ability to dynam-

ically or automatically add participants is also useful.

In-session features include the ability to announce all participants, and for more advanced systems, the ability to incorporate dataconferencing. Unique IDs and passwords for users as well as for conference sessions allows increased security. Security is particularly important, as many of these meetings are unsupervised.

Conference-Intensive Requirements

While these features are reasonable for standard enterprise usage, conference-intensive companies may want to more carefully consider redundant facilities and retain a conference outsourcer for backup and overflow. Enterprises that offer conferencing as part of their underlying service or that use the conferences in a revenue-generating model should look beyond enterprise solutions toward the more-robust conferencing systems used by service

providers. One common issue for these rigorous applications is their ability to provide agent-side reports (reports not just on incoming lines and meetings, but also on the activities of the conference agents).

Bottom Line

- Enterprises can obtain significant savings, increased functionality, and better control by having an in-house conference bridge facility.
- However, enterprises may experience lower service levels, and in some cases, will find an in-house solution, when combined with outsourced backup, to be a viable approach.

Written by Edward Younker,
Research Products
Analytical source: Bernard Elliot,
Enterprise Network Strategies

For related articles published in Point-to-Point, see:

- "CIO Update: Buy Smarter and Better Instead of Less When Networking Budget Cuts Hit," 25 May 2001

Management Update: Time to Tighten Security Measures for Malicious Telephone Calls

Many enterprise executives are quite concerned about security issues, as well as the associated privacy aspects related to heightened security measures. Traditional telecommunications practices give enterprises many tools to track and stop malicious calls. In a new era of heightened security and greater downside risks, enterprises must revisit and reinvigorate these old tools.

Security Concerns

As the world rethinks its stance on security and privacy, certain infrastructure components can greatly assist in increasing security. The telecommunications industry in general and call center, telemanagement and network service provider (NSP) security groups in particular, are accustomed to dealing with security issues. Gartner expects that enterprises will want to place more emphasis on being able to identify, track and stop malicious calls into their sites, regardless of whether they are pranks or the real thing.

One concern is that the new generation of IP-based PBXs and public network soft switches do not have the proven ability to deal with malicious or suspicious calls. Enterprises should revisit their inbound call-tracking capabilities. Vulnerable industries or sites, in most cases, should postpone the migration to IP-based products until the field-proven features appear.

Problem Definition

Ever since the telephone was invented, malicious callers have used it to communicate threats — real or prank in nature. No enterprise can afford to ignore such threats. The telecommunications industry has developed multiple tools to find the calls, track their origination and destination, and, in certain cases, deflect them. The range of threats can be a real bomb notice at worst to false bomb threats of moderate severity to prank calls or unwanted solicitations at the lower end. Each level of malicious call can be handled appropriately via a mix of security procedures and technology.

Gartner expects that enterprises and organizations in the financial services, healthcare, education, higher education, airline and transportation industries will find this advice most immediately useful, but no enterprise is immune.

Traditional Approaches

Three classes of approaches are used to deal with malicious calls that can operate in conjunction with each other for the ultimate security:

- Internal PBX/automatic call distributor features such as malicious call trace and emergency keys enable the recipient or call agent to flag the call or alert supervisors or a security force. Once a call has been flagged, malicious call trace captures the calling line ID, the trunk is

identified and the call is “held up.” Other features can include starting a recorder and notifying security staff. During the recent U.S. national tragedies, even short audio clips from some of the victims have been of interest to law enforcement.

- Telemanagement software and, in particular, real-time monitoring packages with alarm notification and filtering capability have evolved out of the toll-fraud detection industry to deal with inbound threats. Vendors include ISI, MDR Switchview, and MTS IntegraTRACK. Various methods are employed, ranging from simply screening for unusual events to real-time toll-fraud detect-and-disable applications. Alarm-driven pager and cell-phone outputs are also available.
- Various NSPs have evolved dedicated groups and service features to enable them to assist law enforcement and enterprise fraud detection. In some cases, that approach may require Federal Bureau of Investigation or court assistance. This type of approach is particularly essential if an enterprise expects pay-phone-originated, cell-phone-originated or revolving number threats. The most successful enterprises employ a combination of the three approaches to successfully stop personal safety threats and rogue recruiting from competitors.

Management Update: Time to Tighten Security Measures for Malicious Telephone Calls (continued)

Concerns With IP-Based Equipment

Although there are growing reasons to consider IP-based PBXs in the enterprise environment — e.g., less-expensive move, adds, changes; more-intuitive administration tools; long-term total cost of ownership reduction — the ability of vendors to carry over telemanagement and traditional malicious call treatment features to the new products is limited.

Gartner believes this is partly because of the vendors' desire for quick time to market, partly because of not placing a priority on features that had limited use even one month ago, and partly because of more complex routing and tracing requirements, especially in multiswitch networks. For example, the Cisco Systems Call Manager 3.1 does not allow real-time, online call detail

record data. Even hybrid products in which the traditional telecommunications code base is front-ended by an IP platform are challenged to report and track malicious call data as consistently as their circuit-switched forebears do.

Bottom Line

- Enterprises should ensure that all IP PBXs being reviewed fully support malicious call trace and emergency keys.
- Enterprises should enable real-time monitoring packages' features and conduct training at least annually in their use.
- For at least the next two years, each enterprise must evaluate its risks, security priorities and technology plans with an eye toward dealing with a heightened stage of alert.

- Gartner believes that enterprises must learn from the lessons of the past and not ignore the tools that have been developed as a result of such lessons when evaluating voice-switching products.

Written by Edward Younker,
Research Products
Analytical sources: Joe Baylock
and Kathleen Simpson,
Enterprise Network Strategies

For related articles published in Point-to-Point, see:

- "Management Update: Mobile and Wireless Security — Worst and Best Practices," 26 October 2001
- "CIO Alert: Plan for Increased Internet Security After Terrorist Attacks," 26 October 2001
- "CIO Update: VPN Security and Placement," 28 September 2001
- "Management Update: The Gartner 2001 Hype Cycle — Emerging Trends and Technologies," 31 August 2001

Cross Talk

CEO's Departure Ends British Telecom's Worldwide Ambitions. On 31 October 2001, British Telecommunications (BT) announced that Sir Peter Bonfield will resign as CEO at the end of January 2002, nearly a year early. Appointed in January 1996, Bonfield will have held this position for six years. BT has not announced a successor.

Bonfield turned in a lackluster performance as BT's CEO. During his tenure, BT's proposed merger with MCI collapsed when WorldCom outbid BT late in the game. This unexpected turn caused the collapse of Concert, BT's joint venture with MCI. BT then tried to relaunch Concert in partnership with AT&T, but that partnership collapsed as well. Bonfield also oversaw the company as it accumulated its highest-ever debt, with BT's spending heavily on third-generation wireless licenses in the United Kingdom and Germany. BT has continued to lose market share in the United Kingdom, and its share price has fallen back to where it

was when Bonfield became CEO (having risen to record heights in the interim). The early departure of Bonfield shows that BT's board of directors has finally realized that he has taken the company back to where it was in 1995 and that someone else should figure out where BT's future lies. Whomever BT appoints as CEO will face the significant challenge of making BT's culture fast-moving and responsive — one able to make successful acquisitions or merger deals in a restructuring European telecom arena. Bonfield's departure ends the era he presided over jointly with Sir Iain Vallance (Vallance resigned as chairman in April 2001). With a new chairman (Sir Christopher Bland, famous for restructuring the BBC), and once BT chooses a new CEO, Gartner expects a wholesale exodus of senior managers groomed by Bonfield and Vallance. Enterprises should therefore take none of BT's previously announced strategies as given. In particular, Gartner believes BT has ended the push to become a global player. It has now re-trenched to Europe, where it is committed to BT Ignite, its pan-European IP and business solutions service.

Through at least 4Q02, enterprises have a limited choice if they need high-quality global telecom service and want stability: They can use Equant (now part of France Telecom) or Infonet, which is itself up for sale. For pan-European networks, expect BT Ignite to become a welcome, refocused competitor.

Analytical sources: Eric Paulak and David Neil, Enterprise Network Strategies Europe

Prepare for Higher E-Mail Traffic Because of Anthrax Threat. On 25 October 2001, the U.S. Postal Service began trucking mail bound for federal offices in Washington to an Ohio company to be irradiated and to eliminate the threat of anthrax contamination.

E-mail messaging has increased at a compound annual growth rate (CAGR) of 40 percent since 1981. Gartner believes recent events involving anthrax contamination of U.S. mail will increase this rate to 45 percent through 4Q02. Most business mail has already made the transition to electronic media. A Gartner survey in 2000 found that 12 percent of business-to-business invoices among companies with at least \$100 million in revenue were already electronic, and enterprises expected high growth in this area — the figure would reach 40 percent in 2004. Most electronic invoice transmissions are performed through electronic data interchange (EDI) value-added networks, but volume has shifted quickly to Internet channels.

Moving customer-facing correspondence from paper to e-mail has a significant potential for growth. Help desk and marketing have moved a portion of traffic from paper, fax and voice to e-mail. Customer-facing organizations, such as media and political groups, will undergo the most dramatic transition. They will likely outsource the handling of incoming paper mail to shops that will irradiate it and forward electronic images to the addressees.

Handling an upsurge in e-mail of at least 40 percent per year requires serious attention to bandwidth, capacity planning at all switching points and disk space — which should be tailored to the needs of the recipient. Running out of disk space regularly makes handling e-mail tedious and wastes valuable people power. The more people rely on e-mail, the more reliable it must be. Enterprises now have an increased need for business continuity planning and daily screening of all incoming sources. Enterprises must implement solid spam and virus protection at:

Cross Talk (continued)

- All desktops
- The boundary to the Internet
- The messaging server

Anthrax e-mail hoaxes and viruses will likely increase through 2Q02. Since this activity is emotionally disturbing, enterprises should provide terrorist-reaction counseling for both managers and employees.

Analytical sources: Joyce Graff, Maurene Grey and Avivah Litan, *Intranets & Electronic Workplace*

MobileStar's Plight Won't Impact U.S. Wireless Internet Use. Wireless Internet access provider MobileStar Network recently laid off the majority of its employees after the company failed to secure additional financing. MobileStar engaged the Diablo Management Group to determine whether to restructure the company or dispose of assets, and began shutting down its wireless Internet access network. MobileStar was a leader in providing wireless Internet access points at hotels, airports and, most notably, Starbucks restaurants across the United States.

Despite the speed of some pundits to cite MobileStar's troubles as a deterrent to the continued growth of wireless LANs, the long-term impact will likely be minimal. Much of the fixed-infrastructure investment related to installing wireless Internet access points has been made.

Either a restructured MobileStar or a new owner could run most of MobileStar's installations at reasonably low cost. Microsoft and Wayport are the most-mentioned potential buyers of the company. Through MSN, Microsoft already has a partnership with MobileStar at Starbucks. Wayport, a direct MobileStar competitor, could extend its market reach by acquiring these installations.

Although wireless Internet access is not ubiquitous, enough access points exist in airports and hotels to provide real advantages to business travelers. Wireless modems cost less than \$100.

Enterprises should consider purchasing wireless modems and monthly wireless Internet services to increase productivity of their mobile professionals. With increased security making much longer lead times a permanent reality for air travel, wireless Internet access makes even more sense than ever for those who have rigorous business travel schedules.

Analytical source: Leslie Fiering, *Hardware Platforms Worldwide*

China Takes Next Step Toward Telecom Competition. On 16 October 2001, the Chinese government announced its decision to split its fixed-line monopoly, China Telecommunications, into two regional companies along roughly north-south lines. The company's assets in 10 northern and coastal provinces and cities will merge with China Netcom, the only Chinese telecom firm with direct foreign investment.

The government's decision will disappoint those hoping that China would break up China Telecom along functional or business lines to increase competition. A simple regional split does little to encourage competition, and it does nothing to bring new competition to the key area of local-loop access. In effect, one virtual monopoly has given way to two. However, this restructuring marks stage two of an ongoing

process rather than an end in itself. Stage one began with the creation and listing of China Telecom in Hong Kong in 1997, which eventually led to the total separation of China Mobile from China Telecom. During this time, China learned how to package and sell attractive mobile assets to international investors through the equity and bond markets without ceding control or letting outside interests have any say in running the businesses. This model that worked well, and the government hopes that the fixed-line business will go through the same process.

Initially, the government thought China Telecom (or some of its assets) would be publicly listed during 2000. However, the difficulty in parceling up such a huge company forced another approach. The creation of two new smaller companies offers the chance to serve up investment opportunities that the world's capital markets can more easily digest. The merger of Netcom into the northern business of China Telecom allows Netcom to seek corporate and long-distance customers in the south. At the same time, China Telecom's southern area will receive one of the new mobile licenses, allowing it to compete in the north. In short, these provisions represent the beginnings of multiservice businesses for both companies, which, in time, will become competitive.

As multiservice businesses emerge, enterprises should be able to leave their contracts easily to contract for service from other operators, and they will have a greater choice of operators and products. At this second stage of an ongoing process, however, enterprises should not expect the benefits of a competitive environment to develop until at least 2004.

Analytical sources: Andrew Chetham and Margot Hooley, Enterprise Network Strategies Pacific

Network Associates Throws Down Gauntlet. On 12 October 2001, Network Associates Inc. (NAI) announced that it will integrate its PGP security business unit into the McAfee and Sniffer units. NAI will sell or close down its desktop security tools, including desktop encryption, e-mail, encryption tool sets and the Gauntlet firewall. NAI will integrate the distributed firewall, CyberCop vulnerability assessment tools and e-business server technologies into McAfee and Sniffer to develop comprehensive security offerings.

NAI acquired Gauntlet through its purchase of Trusted Information Systems. The once-dominant firewall product suffered through several business-strategy shifts within NAI while the firewall market space went through a dramatic growth phase. Check Point Software Technologies and Cisco Systems became the market leaders, and appliance firewalls have now made it almost impossible for software-only firewalls to survive. NAI's relatively new upper management has taken a hard look at actual results and wisely decided to move on. Gauntlet still has a good brand name, and NAI may have some success at selling it — although ongoing customer support may be too daunting for a suitor to undertake. The PGP desktop security products have suffered from a different set of problems. While Gauntlet was an unappreciated product in a booming market, PGP encryption tools were highly valued products in a market that did not materialize. The other encryption vendors have seen a similar lack of demand and are restructuring to focus on products that sell, such as enterprise access management and staged-server secure messaging services, which rely on Secure Sockets Layer. NAI will likely find a buyer for PGP desktop encryption tools. The technology is good, and the installed base will have ongoing support.

Cross Talk (continued)

Enterprises with Gauntlet firewall-based perimeter defenses should begin to investigate replacement technology. Although NAI has committed to supporting its customers, the abundance of activity in network security will likely affect the company's ability to support a product that has reached end of life.

Analytical sources: Richard Stiennon, Vic Wheatman and Joyce Graff, Information Security Strategies

Converged Networking Will Still Grow Slowly Without ION. On 17 October 2001, Sprint announced that it plans to terminate its ION converged voice and data network services. Sprint will transition ION customers to other network services.

The demise of the first major converged network services (CNS) initiative by a major network service provider does not mean the end of CNS itself. CNS will become mainstream — just not right away. ION did not succeed for reasons particular to Sprint as well as trends retarding the development of the whole CNS market. The failed merger with WorldCom distracted Sprint. Also, ION had problems delivering stable voice quality, especially to small sites. The industry trends hurt even more. Sprint built ION on an asynchronous transfer mode (ATM) platform, but now the market has swung over to integrating voice and data networks on IP. It made sense for Sprint to halt further investment in ION. In addition, when Sprint introduced ION in 1998, U. S. enterprises could save 25 percent or more on networking costs by running voice over a data network. Since then, the rapid decline in the price of traditional long-distance services has cut ION's advantage to 10 percent or less. Enterprises still want to implement CNS, but they now have more urgent networking priorities such as dealing with the aftermath of the terrorist attacks on 11 September 2001 and supporting e-business.

CNS has the greatest cost advantage for international service because of relatively high voice charges among many countries. Through 2005, enterprises will principally deploy CNS to lower the cost of multinational networks (0.8 probability). Accordingly, CNS will have slow uptake by enterprises generally, but adding CNS will not significantly boost the cost of major network upgrades. Therefore, through 2005, most enterprises will implement CNS when upgrading their networks for other reasons (0.8 probability).

Sprint stated that it will transition ION customers to traditional voice and data services as smoothly as possible, but any such transition carries some risk. Enterprises should ensure that Sprint follows the same terms and conditions for the new services as agreed to in its ION contracts — e.g., on prices and service-level guarantees. Enterprises should also seek commitments from Sprint that it will make the transition to new networks as transparent as possible for enterprise systems.

Analytical source: Jay Pultz, Enterprise Network Strategies