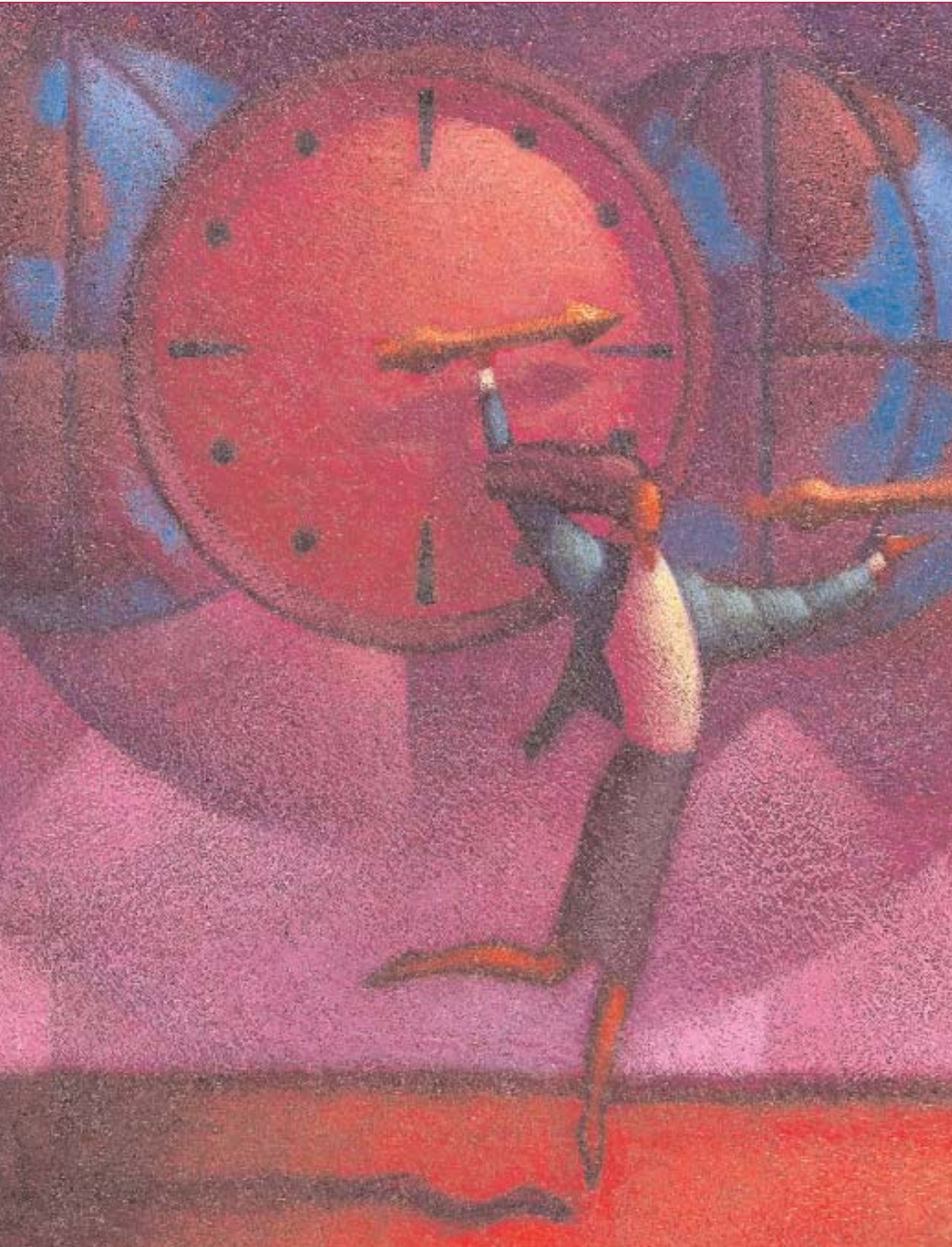


Creating Omnipresence *Through Telecommunications Technologies*

November 2005



i/+^ International Legal
Technology Association
Peer Powered

A Publication of ILTA

About ILTA

Providing technology solutions to law firms and law departments gets more complex every day. Connecting with your peers to exchange ideas with those who have “been there, done that” has never been more valuable.

For nearly three decades, the International Legal Technology Association has led the way in sharing knowledge and experience for those faced with challenges in their firms and legal departments. ILTA members come from firms and law departments of all sizes and all areas of practice, all sharing a common need to have access to the latest information about products and support services that impact the legal profession.

ILTA’s Statement of Purpose: ILTA is the premier peer networking organization providing information resources to members in order to make technology work for the legal profession.

Editors’ Note

Alexander Graham Bell once said, “Leave the beaten track occasionally and dive into the woods. Every time you do so, you will be certain to find something that you have never seen before.” Little did he know, many have since left that beaten path to find new and ingenious ways to take advantage of his little invention. We’ve moved from needing the assistance of an operator to place a call to a time when worldwide teleconferences are commonplace.

We’ve called on our authors to share their knowledge and expertise on telecommunications technologies. We’ll look at new WAN performance capabilities, the merits of a move to IPT, what types of videoconferencing are best for you, and how to keep it all secure. Thanks to the authors for taking us “off hold” and moving us forward.

Thinking about Mr. Bell’s first telephone conversation, “Mr. Watson, come here; I want to see you,” if he had just waited another 125 years, he could have seen him with just a click of the mouse.

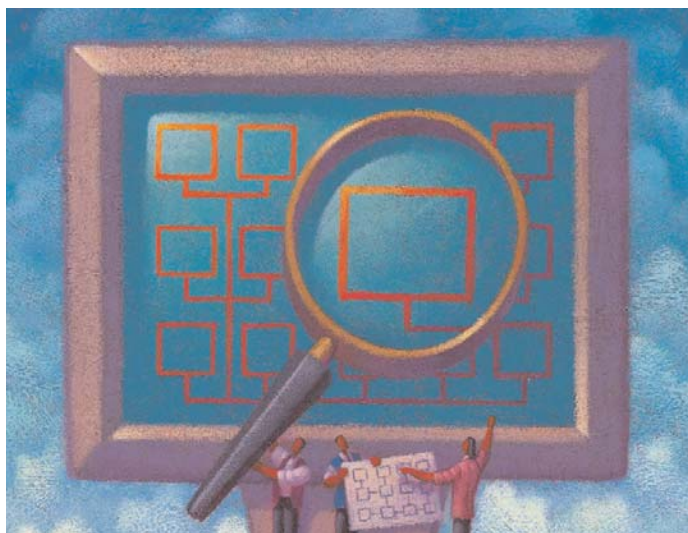
Ken Hansen and Randi Mayes, Editors

Table of Contents

| | |
|---|----|
| Securing Telecommunications: Mission Impossible? | 3 |
| by Faith M. Heikkila and Kristen Zarcadoolas of Pivot Group | |
| Making the Move to IPT | 7 |
| by Athelene Gieseman of Stinson Morrison Hecker LLP | |
| Presence Technology - A Boon to Communication | 9 |
| by Roger Bonine of Miller & Martin LLP | |
| Global Attorneys, Centralized IT: A New Approach to WAN Performance | 11 |
| by Apurva Davé of Riverbed Technology | |
| Auto-Capture Time on the Phone | 14 |
| by Ray Deck of Element 55 | |
| Creating Omnipresence Through Video Technology | 16 |
| by Jack M. Sheekey of VideoTeleCon | |
| Understanding Your Wireless Needs | 20 |
| by Berylle Reynolds of MBR Wireless Consulting | |

Securing Telecommunications: Mission Impossible?

by Faith M. Heikkila and Kristen Zarcadoolas, Pivot Group



An attorney from your law firm is in the airport and needs to pull up the client's pricing contracts from the litigation support database located on the firm's servers. Using a Wi-Fi hotspot in the airport, the attorney runs a search of the litigation support database, finds the highly confidential document and downloads it to the laptop. While connecting to the firm's network via the Internet, a rogue user piggybacks on the lawyer's connection and gains unauthorized access to the law firm's network. Upon entry, the unauthorized user starts to download sensitive and confidential documents showing the social security numbers, addresses and earnings of employees of one the firm's Fortune 500 clients.

As this scenario depicts, the pervasiveness of telecommunications available to lawyers has made information security of utmost importance in protecting the attorney-client privilege, the work product doctrine, as well as the confidentiality, integrity and availability of documents. According to ILTA's 2004 Technology Survey of 446 law firms, "Remote access is ubiquitous. Virtually all firms (99.6

percent) now provide some form of access from outside the firm to e-mail, documents and other applications stored inside the firm." This remote access could compromise the security of a network should a hacker or other unauthorized person connect to this information as demonstrated above. In a law firm or law department setting, the intruder could gain access to attorney-client privileged documents that may contain proprietary information, trade secrets, shareholder information or other private data that may be damaging to a client, as well as the law firm, if it were to become public.

Telecommunication Flavors

Since remote access is now considered universal, it is important to understand the various forms of telecommunications available. A law firm may use a combination of connectivity options, and the choice of telecommunications mode will depend upon the needs of the entity, cost of deploying the selected technology and the security impact of such deployment.

Law firms and law departments utilize broadband networks to allow their employees and clients access to data. Telecommunications provide the ability to communicate from a distance outside of the office and gain access to an entity's local area network (LAN) or wide area network (WAN) in order to access files. Telecommunications through the Internet, extranets, virtual private networks (VPNs), digital subscriber lines (DSLs), cable modems, dial-up, wireless, Application Service Providers (ASPs) or other network connectivity solutions connect authorized users to the organization's data.

Connectivity of remote offices is typically achieved by a combination of T-1 leased lines equivalent to 1.544 Mbps, T-3 dedicated lines with rates up to 43 Mbps and/or Optical Carrier-3 lines capable of 155.52 Mbps. Smaller law firms tend to rely on DSL lines and/or T-1 lines. Large law firms commonly use Asynchronous Transfer Mode (ATM), Ethernet, Fast Ethernet, or the newer Gigabit Ethernet to connect their office servers.

With regard to attorneys, paralegals and support staff who need to connect to the organization's network from home, there are a number of telecommunications technologies available. According to M. K. Littman in *Building Broadband Networks*, the first-mile connectivity from the user's home to the office is contingent upon the bandwidth rate available from the consumer's home to the Internet Service Provider's (ISP) office. Optical fiber broadband networks are currently being

installed throughout the country. Optical fiber provides a higher bandwidth capability with speeds of 100 Mbps for fiber-to-the-home (FTTH) and up to 1 Gbps in fiber-to-the-business (FTTB). High bandwidth connectivity options have improved substantially for the home user. Cable modems provide instant-on connectivity through the local cable television company. The advertised transmission rates are up to 3 Mbps upstream in some areas. The DSL options for home users and businesses have also grown significantly over the past few years by using existing public switched telephone networks (PSTNs) for data transmission. These transmission rates are comparable to cable transmission rates. Thus, DSL provides an alternative to cable connectivity.

Attorneys also utilize laptops, Blackberry devices, PDAs and/or cell phones to connect to the office e-mail system from away from the office. Voice over IP (VoIP) and instant messenger (IM) are also new technologies being deployed by law firms. The question to be answered with any and all of these telecommunications technologies is, "How do I ensure that my telecommunications choice does not adversely affect the security of our network?"

Necessity and Benefits of Information Security

With the growing number of options in telecommunications and any combination thereof, the number of threats and vulnerabilities an organization faces is alarming at best. Without any information security program in place, law firms and law departments risk losing billable time and revenue to telecommunications downtime, higher IT costs for replacement or repair after an incident and regulatory compliance violations.

As more companies get caught in the crossfire of security-related incidents with mass media coverage, clients are becoming more savvy when it comes to the security of their assets and demanding superior protection and quality of service. This puts a firm's reputation at stake, should the trust the client places in the firm suddenly be shattered due to an inadvertent or deliberate disclosure of the client's information to unauthorized parties. The exposure to the firm could range in the millions of dollars and/or severely damage the firm's reputation.

Therefore, the cost of not implementing information security measures around telecommunications far outweighs the cost of incorporating such measures in the short-term and the long-run.

Securing telecommunications can quite easily become a business enabler and competitive advantage when the following benefits are considered:

Increase in productivity

Protection of assets

Mitigation of loss

Minimization of penalties and fees

Telecommunications and Information Security

Vulnerabilities abound: Viruses, worms, malicious software, well-known Web browser vulnerabilities and Microsoft IIS server vulnerabilities, spyware, Trojan horse programs, keystroke loggers, rootkits, ransomware, wireless network intrusion, unauthorized wired network access buffer overflows and denial-of-service (DoS) attacks must all be guarded against when employing telecommunications technologies. Eavesdropping and tampering with the transmission of data across the Internet, extranets and intranets by unauthorized users are vulnerabilities of telecommunications of which organizations should also be aware.

Unencrypted data transmitted using a telecommunications technology is at risk of unauthorized retrieval by disgruntled employees or unknown intruders. The curious or malicious person may attempt to access documents or e-mail messages. The sensitive information being intercepted could bring a nefarious person an incredibly large sum of money if they were to sell it. This is a high risk threat, and controls must be put into place to protect against it.

What are the security technologies available for telecommunications methods?

Identify the business assets that need to be protected. In law firms and law departments, the confidential and sensitive client documents, as well as the attorney-client privileged and work-product doctrine documents must be safeguarded. Defense-in-depth is a critical component of managing and monitoring an organization's network. In order to protect the tangible assets of electronic documents, software and hardware, the law firm or law department needs to implement firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), encryption and access controls. Cryptographic protocols and applications should implement Transport Layer Security Protocol (TLS) — the latest Secure Socket Layer (SSL) — to encrypt messages in real time and prevent eavesdropping. Internet Protocol Security (IPSec), Secure Shell (SSH), and Pretty Good Privacy (PGP) all provide cryptographic measures for securing telecommunications.

For wireless networks, 802.11 Wired Equivalent Privacy (WEP), 802.11i Wi-Fi Protected Access (WPA) and Advance Encryption Standard (AES) with a key size of up to 256 bits

are examples of defense-in-depth security technologies used to protect telecommunications methods. Currently, WEP is too easily cracked; with the tools of hackers, it can be cracked within four minutes. With the lack of key management and user authentication, WEP is more vulnerable to hackers using dictionary attacks. Wi-Fi Protected Access (WPA) has improved authentication through the use of temporal key integrity protocol (TKIP) which scrambles each and every frame using a hashing algorithm. After 10,000 packets, the encryption key changes. The Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) takes 128 bit key blocks of data through the AES encryption standard. CCMP uses WPA1 and WPA2 to allow for a quick handoff cipher block with 128-bit encryption that will eventually evolve into the next 802.11i standard.

Physical security is another layer of defense-in-depth that includes reviewing the physical components as well as the telecommunications element that could be susceptible to any potential threats to an organization's business assets. In our scenario of an attorney using a Wi-Fi hotspot at the airport, the physical security of the laptop must remain under the watchful eye of the attorney. Furthermore, should the attorney forget the laptop at the airport screening area, the laptop should be encrypted using at least AES encryption. A two-factor authentication would also be advisable, whether it is a biometric scan, token or smartcard. This will ensure that there are protections in place should someone steal the laptop off the scanning belt.

How will security tools fit into a law firm's or law department's telecommunications technology architecture?
The use of multi-layered security tools will provide the defense-in-depth necessary to ensure an acceptable level of security for the organization's telecommunications technology architecture. An intrusion prevention system (IPS) is a real-time prevention system that blocks attacks as they happen. IPS is a proactive technology that deals with network-based threats against service, such as spyware and buffer overflows. The value of an IPS on laptops is that it generates alerts showing what IP addresses are infected and assists with an incident response. While IDS is more reactive than proactive, it still provides another layer in protecting law firm and law department networks.

Locking the front door to the office so that an intruder cannot enter is a typical method of securing the office. Many entities take it a step further by requiring something you have and something you know — an access card or the numbers for the combination lock on the door. The same holds true with the physical access to law firm computers, servers, laptops,

BlackBerry devices and cell phones. Two-factor authentication of “what you have” assists with authenticating who you are and “what you know” for computer access control. Two-factor authentication can be achieved by tokens, where the generation of a new code occurs every 60 seconds. Biometrics is fairly new. However, some of the new laptops are coming out with a thumbprint requirement in order to access the laptop.

How easy or difficult will it be to implement and maintain a security structure around telecommunications systems?

The security structure will involve many different technologies of varying complexity. Technologies may not be manageable from a central console and should be deployed in a sequential manner. However, trying to implement everything all at once is not be feasible in most cases. Many components will require user training which will assist in appropriate implementation. Installing a security technology and forgetting about it is not an option; proper security measures cannot be maintained in that manner. Thus, the most prevalent difficulty is the constant vigil necessary to monitor, upgrade and analyze data on a continual basis.

What is the trade-off in securing telecommunications as far as security, performance and resources are concerned?

Firewalls, intrusion detection/prevention systems and encryption can slow down the performance of a network. With higher bandwidth networks, it is critical to the end user that security measures not equate to a degradation of the throughput of the connection. Encryption and decryption can be tedious if the telecommunications bandwidth speed of downloading and uploading documents is adversely affected. Therefore, consider the potential performance impact of deployment of such systems and ensure the models that can handle the expected network load are used. Another alternative is to incorporate cryptographic accelerators to increase encryption/decryption performance.

Putting It All Together

Let's look at an example of implementing and securing VoIP. VoIP allows for the transmission of voice calls over packet-switched IP networks rather than through the analog PSTNs. Some considerations and investigation are merited when considering implementing a secured VoIP system in the law firm or law department environment:

1. **Security issues include wire tapping, eavesdropping and hijacking of telephone calls.** All network threats that are prevalent in data networks, including, but not limited to, packet sniffing, man-in-the-middle attacks, phishing, DoS attacks, viruses, worms, Trojans and spam are also of enormous concern with VoIP.

Encryption of the VoIP network is essential to protect against the monitoring of telephone conversations. Encryption is now available in AES and can be done in block cipher or stream to protect the privacy and authenticity of the call.

Firewalls must protect the gateways, routers and endpoints.

Wireless telephone usage with Voice over Wi-Fi (VoWi-Fi) can be utilized on laptops, cell phones and PDAs. VoWi-Fi should include the 802.11i Wi-Fi Protected Access standard to encrypt conversations and provide some protection from hackers intercepting calls.

If VoIP and data are run on the same network, there is a risk that a data traffic spike will cause delay or loss of enough VoIP traffic that the sound/video quality will be diminished. It would be best to separate the traffic if affordable. The reason for segmentation is data network traffic is “bursty,” meaning that there are traffic spikes periodically. However, if separation is not cost-effective, then the occasional degradation in the quality of the real-time VoIP sound/video will be a slight inconvenience. Separating the two streams also shields the VoIP network from all of the broadcast and multi-cast traffic seen on LANs recently.

2. **The quality of service (QoS) must meet users’ expectations.** Calls must take precedence over data. Emergency 911 services must also be addressed since 911 calls are traced back to a user’s location. With VoIP, the user’s location is not necessarily known. This service should be addressed with the VoIP vendor. Since wireless phones can be utilized with VoIP, wireless security issues are prevalent just as they would be in data networks. Replacement of the call center to assure that special functions such as call forwarding and teleconferencing continue to meet user expectations should also be examined. Interviews of every practice group and business unit to ascertain their special telephone needs would assist with meeting user’s QoS expectations.
3. **Bandwidth issues are exponentially increased.** Attention should be given to packet size, and calculations should be made based on the percentage of people on the phone at any given time. Bandwidth should be accordingly increased to avoid congestion and latency (the time it takes the call to go from the caller to the recipient) in delivering phone calls.

4. **Redundancy of servers and load balancing is another key consideration.** Fax machines can be impacted as most fax machines and scanners are analog while VoIP utilizes digital signals. Analog to digital signal converters are available, and the costs of purchasing this hardware should be a consideration.
5. **Around-the-clock maintenance and support from the VoIP vendor is crucial to keep the VoIP system up and running.** The vendor’s call support center should have a spare system in stock for the organization’s VoIP system at all times. There should be a two-hour window for delivery of a spare system in order to keep the organization functional. In the event that the VoIP system fails, there should be a backup plan to rollback to the analog phones. It would be wise to keep the analog telephones on employees’ desks during the deployment of VoIP for a quick transition back to analog during a rollback.

The points above highlight the main security issues and other concerns to address in the planning phase of employing the telecommunications technology and VoIP in a law firm environment. It should be noted that while certain aspects may not fall directly under the “security” section, it is reasonable to deduce that each one has, in some fashion, its own security obstacles.

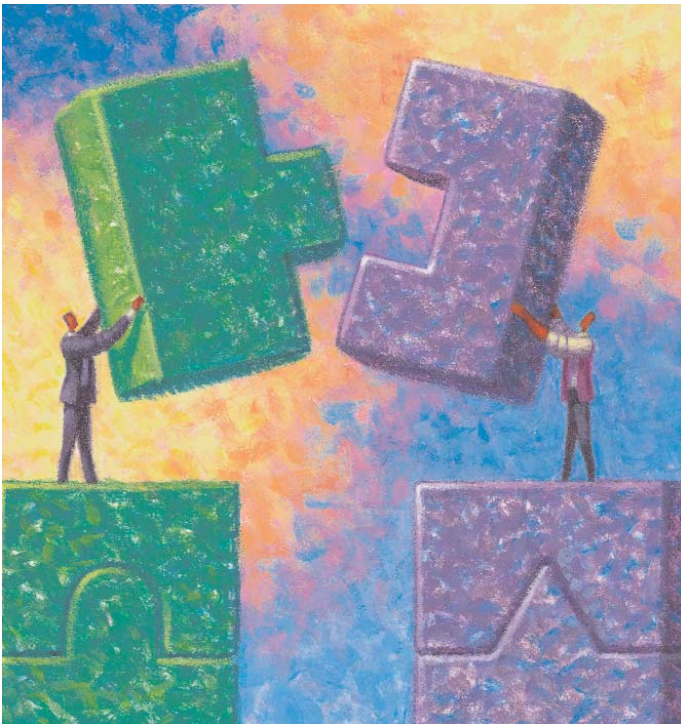
Mission Possible

As illustrated, information security is critical to the success of any well-designed implementation of telecommunications within the workplace. Precautionary steps must be taken to protect the critical assets of a law firm and its clients against the volatile nature of data exchange over open space. Therefore, it is important to first look — identify the critical assets and assess the firm’s risk. Next, plan — develop a proactive security program wrapped around the telecommunications technology selected as well as the current system and network architecture. Then, act upon the chosen program swiftly — implement a firm-specific tailored information security road map properly (including policies, training and technology). Once the overall plan has been put into action, repeat the entire process with on-going monitoring, auditing, updating and adjusting to business and technology changes.

Secured telecommunications can, and will, be a significant competitive advantage and an essential business enabler for the legal arena when built with the appropriate tools and knowledge.

Making the Move to IPT

by Athelene Gieseman of Stinson Morrison Hecker LLP



Stinson Morrison Hecker LLP began its implementation of a 1,000-phone IP telephony (IPT) system in 2002. We were pioneers at that time, and given our Midwestern presence, it seemed rather fitting. Just like the original pioneers, the trail was sometimes treacherous. So was it worth it?

That May, Morrison & Hecker L.L.P. and Stinson Mag & Fizzell, P.C. combined. As many firms that have done this know, the primary focus after such a combination is bringing people together and creating a new culture. In our case, there were many things we did to ensure that the technology did not impede that process. In fact, the goal was to use technology to enhance the process. For example, our networks and document management systems were unified by mid-May and our e-mail systems by August.

During the planning stages of the combination, we identified a significant difference in our phone systems. One firm was using a Siemens phone system which had basic networking between offices, and the other had various phone systems for each office — not networked. Given the importance of

phones to attorneys, we knew we had to create one system as quickly as possible.

In our search for a new system, we looked at traditional phone systems (circuit-based switching), as well as IP systems (packet-based switching). An extensive ROI was done to determine which system was most cost efficient. Our return on investment using an IP system was conservatively determined to be five years. We did not take into account any opportunity costs we would gain from features like extension mobility and SoftPhones (which allow an attorney superior and easy-to-use access to their phone while out of the office). We also evaluated the flexibility of each type of system for future growth.

Traditional System Findings

Circuit-based switching was attractive for one important reason — we knew it. We had staff who had used and managed it for years. Our users were familiar with the features and functions of traditional systems. But there was a down side. One problem with traditional phones is they require a huge amount of care and feeding for routine tasks such as moving a phone from one room to another. Using IPT, we were able to move approximately 250 people from one building to another in one weekend without making a single change to our phone system.

Why We Chose IPT

We discovered that most traditional systems were not as feature-rich as their IPT cousins, and the cost of maintenance is very high. Features such as extension mobility, advanced conferencing, follow-me-features and SoftPhone were not part of a traditional environment. Further, we knew the industry was moving toward IPT and development efforts would be focused on the new technology. Why purchase a system that would be outdated almost the day it is installed?

With IPT, the systems are very scalable. One server can support up to 2,500 users and cost less than the one board upgrade for a traditional switch. A three-office upgrade for one of the traditional systems to the latest software release would have cost \$85,000.

Another consideration was the cost of infrastructure upgrades. Upgrading wiring, routers and switches can be daunting. In our case, we needed to address our disparate infrastructure. By using standards-based equipment and software at each office, along with a single management package, you can

properly ensure quality data support for your firm or law department. While data is not always considered to be as important as phones, that landscape is quickly changing. All of our communication systems, such as e-mail, have become “must have” applications. It is important to have a solid infrastructure for data as well as voice. In our case, we needed to fix that problem regardless of our telephony needs. As we upgraded our data network, we architected so that we could easily run IPT on it.

The great promise of IPT is to move our telephony world to a standards-based environment. Most vendors today are developing systems using the SIP (Session Initiation Protocol) standard. By using this standard, we will be able to use multiple vendors’ components in one system. Remember when computers were proprietary and not standard? If so, you will also remember that you could not buy a drive or a memory card for that system except from the original vendor. Therefore, the demand and cost were high. With a standards-based PC, we are able to purchase various components and software packages to use. IPT is the same. For example, Stinson Morrison Hecker (SMH) leases its phone system. At the end of each lease period, we evaluate which parts of the system we keep, and which we upgrade or replace with a competitor’s product. Because we are now an IPT customer, we have many more options. There won’t be a need to do a fork-lift upgrade to get the improvements or new applications we want. With a truly SIP compliant system, you can purchase any SIP compliant phone. You won’t need to go back to your vendor for a very expensive, proprietary phone, and if another vendor happens to come out with a great new handset, you won’t have to wait for your vendor to get on the bandwagon.

The Implementation

If you have ever been an early adopter of technology, you know that the implementation process can be difficult. Our firm opted to work through those difficulties to gain the benefits and promise of IPT. When we installed our system, we discovered that Cisco’s system was designed to have a switch in each building that worked independently of others. However, SMH wanted all of our offices working as one. We wanted callers to be able to reach anyone in the firm with a single phone call. Many “engineering specials” (ESs) later, we were able to accomplish this. Another challenge was in the area of redundancy. SMH had two large offices in Kansas City as a result of the combination. We wanted to have one switch in each office and have one office backup the other in the event of a failure. While Cisco had done this very successfully on a single-building basis, it had not been done over a wide area network. After a few more ESs, we were able to make this happen. One of the benefits gained is what we call “follow the sun” switchboard coverage. SMH has

offices in three time zones. Because our system is a truly unified system, we can have switchboard operators accept inbound calls from any office. They can also use the overhead paging system in any office, and it allows our main telephone numbers to be answered by a live person from 8:00 a.m. Eastern until 6:00 p.m. Mountain.

Another problem we encountered early on was the feature set of the system. While it had many new features we didn’t have previously (*e.g.*, extension mobility and call directories), it lacked an intuitive user interface. During the past three years, Cisco has taken input from its customers and made significant changes. Attorneys who have left the firm tell me the one thing they miss is the feature set of our phone system.

While the technology itself was somewhat challenging in the early part of our implementation, the most difficult process was training our users in the use of the new system. Those of us who implement technology know that our users are not thrilled with change. But the phone is a device that they expect to always know and understand. The change to an IP system can be challenging to them simply because it has more capabilities. We underestimated the impact of changing the voice mail system. Our attorneys and staff had memorized every keystroke for listening and managing their voice mail. Introducing a new system with new voice prompts was very unsettling to many. Although our users loved being able to check their voice mail from Outlook, they were sometimes confused about the management of messages.

End of the Trail

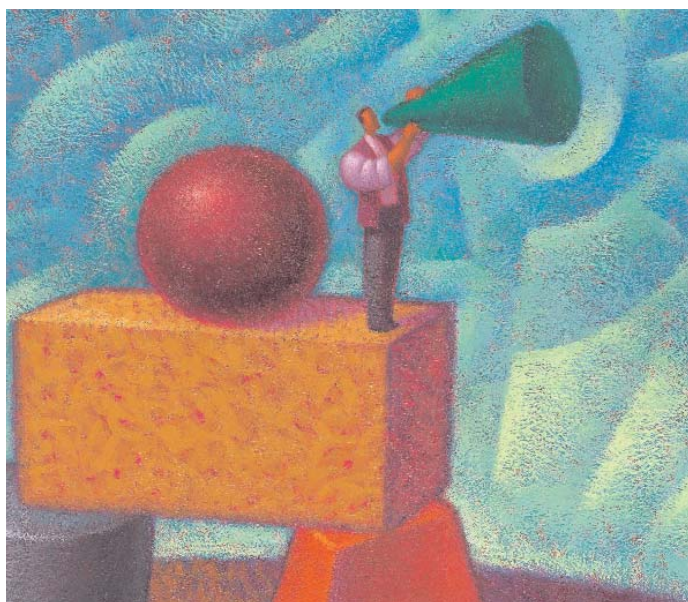
While we’ve had our share of pain blazing the trail, in the end we have a very flexible, feature-rich and reliable system. If we could hit rewind, would we do anything differently? Definitely. We wouldn’t rush the install. We’d do a better job of understanding how our people used their traditional phones. And we’d provide better training. But we would still be an IPT firm.

As we look to the future, we are prepared to offer our users even better communications tools. Wireless phones, presence-based applications, Web applications on phones and a PC used as an office phone while on the road are real applications that we can use. At the end of each lease period we will take advantage of the flexibility of our system and make improvements with no need to throw out the baby with the bath water.

To learn more about using IPT, join ILTA’s Telecom Peer Group. There you’ll be able to gain knowledge and share with others who have already made the change.

Presence Technology — A Boon to Communication

by Roger Bonine of Miller & Martin LLP



Law firms and law departments have seen many changes in communication methods in the past fifteen years. In the early 1990s, Internet e-mail joined the telephone as a critical business communication tool — marginalizing the fax machine in the process. Later, tools such as Web conferencing and videoconferencing provided acceptable alternatives to the fly-in, fly-out business meeting.

Today another technology, known as presence, is looming on the horizon. In the most basic sense, presence technology is a method for determining the current location and availability of someone. Users can broadcast their current whereabouts and status to a centralized server, which then makes this information available to presence-enabled applications.

It's difficult to overstate the usefulness of presence technology. It increases productivity by reducing the occurrence of "phone tag," fosters team relationships for geographically separated users and ensures that critical information can be delivered to the proper people in a timely manner.

While many vendors are busy building presence support into their products, our focus will be on Microsoft and its vision for presence in an enterprise environment.

Live Communications Server 2005

The core product of Microsoft's presence strategy is Live Communications Server 2005. This server platform, which we'll refer to as LCS 2005, provides the infrastructure necessary to share presence data between applications and users on your internal network, and it supports the creation of federated relationships between organizations. For example, using LCS 2005 and federation, your organization and largest client could set up trust relationships between your respective internal IM systems, allowing directory information to be exchanged and communication to occur across company boundaries.

LCS 2005 uses an industry-standard protocol, Session Initiation Protocol (SIP), to create, manage and terminate real-time communications sessions. These sessions aren't limited to text; they can also include voice or streaming video, and it's possible to move from one of these options to another within the same session. This allows users to collaborate in ways that were previously difficult — or impossible.

Microsoft Office Communicator 2005

The flagship presence client for LCS 2005 is Microsoft Office Communicator 2005 (MOC). As you might expect, MOC is a close cousin to Windows Communicator. However, its feature set is geared toward corporate rather than personal use. The most notable example of this is its built-in integration with PBX systems. When used with a supported telephone system, MOC can obtain near-complete control over telephone functions. For example, it can be used to place calls, forward an existing call or set up a conference call. All of these functions can be performed simply by right-clicking on the appropriate icons in your contact list.

When an incoming call is received, MOC can be configured to pop up a notification window. From this window, you can answer the call or instantly divert it to another number, such as your mobile phone. Incoming calls can be automatically forwarded based upon presence information. For example, the system could be instructed to route calls to your mobile phone whenever you are listed as "out of office" in MOC. Your telephone system will need to provide a SIP-to-PSTN (public switched telephone network) gateway to take advantage of voice integration, but most IP and traditional PBX vendors offer this capability.

MOC can also reference free/busy information from the Microsoft Outlook calendar. This, in conjunction with its telephone support, allows much more descriptive information

of a contact's whereabouts. For example, MOC might automatically display "On the telephone," or "In a meeting," rather than the generic "Busy" indicator found in Windows Messenger. If a user has an out-of-office message set in Outlook, the message will appear as an icon on the MOC contact list. Also, if you want to be notified as soon as one of your offline contacts becomes available again, you can tag his or her contact record for notification, and MOC will notify you the moment that the contact comes back online.

Office Applications

Microsoft has built limited presence support into its Office 2003 application suite. In Microsoft Word, for example, typing a name from your contact list causes a smart tag to appear. The smart tag menu will display the online/offline status of the contact and will allow you to instant message, telephone or e-mail the contact from within Word. Outlook and Excel also provide presence information for contacts via smart tags. In SharePoint, it is possible to select a document and see a list of users who are working on the document, along with their presence information.

Future Products

The next version of Windows, Windows Vista, is expected to include built-in presence support when it ships in 2006. A new feature of Vista, code-named "Meeting Space," will use presence information, along with peer-to-peer networking capabilities, to allow users to create temporary workspaces where they can simultaneously edit documents and share files without requiring Web conferencing software such as Live Meeting or WebEx. In an effort to further extend the reach of presence information, Microsoft has also committed to provide an LCS client for BlackBerry devices.

To allow third-party developers to add presence support (and interestingly, telephone integration capability) to their own applications, Microsoft recently announced plans to deliver the RTC Presence Toolkit.

Typical Scenarios

As mentioned earlier, the wide availability of presence information will allow communication in ways that were previously difficult or impossible. Consider these scenarios:

Sam needs to consult with Bill about an urgent document as quickly as possible, but Bill is meeting with a client. Sam tags Bill in Office Communicator and is notified as soon as Bill returns to his desk.

Amanda is in a hotel room at a client site but needs to work through contract revisions with the general counsel of the firm's largest client. Two other firm

attorneys, one in Seattle and one in Boston, also need to be involved in the editing process. By checking the presence information in her contact list, Amanda sees that two of the three remote participants are available; the other is on the telephone. She uses Meeting Space to set up a conference call and shared work area with the two available participants and tags the third. When he hangs up the telephone, he is automatically invited to join the Meeting Space session. The document is brought up for revision by Amanda, and each individual can participate in the editing process.

Rafael is connected to his office via VPN at a coffee house. Office Communicator alerts him that a client is calling his office phone. He has set up filtering so that office calls from some of his contacts are rerouted automatically to his mobile phone when he is offline, and although this particular caller is not one of those "favored" contacts, it is still important that the call be taken immediately. Rafael clicks on the popup message and reroutes the call to his mobile phone, which begins to ring at once.

Areas of Concern

As with any new technology, there are tradeoffs involved with the use of presence. First and foremost, users may be concerned about privacy issues. Information exposed through presence technology may not be appropriate for all potential viewers, especially when trust relationships between two different business entities are considered. Also, not all users are likely to be comfortable with the idea that their whereabouts can be monitored, however loosely. Depending on firm culture, the benefits of increased access may be outweighed by the perceived loss of privacy. In any event, the IT department will need to be cautious in making a case for the benefits of presence technology to ensure successful adoption.

What's Next?

While presence technology is obviously not a good fit for every firm or law department, it is an area that has a high potential for growth. Some technology analysts predict that presence-based IM systems will eventually have market share comparable to that of today's e-mail systems. That day will not arrive for a long time — if ever — but legal IT departments would be wise to keep this technology on their radar screens.

Global Attorneys, Centralized IT

A New Approach to WAN Performance

by Apurva Davé of Riverbed Technology



The legal industry has moved rapidly from small, fragmented firms to a model of consolidated organizations with many practice groups that serve a broad range of clients. Even firms with a just a few offices in one region regularly serve national and global clients. Practice groups are often located in one office, yet they must collaborate frequently with attorneys in different offices. Interoffice client teams are now the norm, yet the architecture of the IT systems that support these teams has not adapted to this new environment.

This dramatic shift in attorney collaboration is causing ripple effects in the utilization of the wide area network (WAN). In the past, the WAN was used for occasional file transfers and scheduled back office IT tasks. Now, however, the WAN is pushed to enable interoffice client teams to work together seamlessly, regardless of practice group or attorney location. For example, a tax attorney based in Seattle may partner with a real estate attorney in Shanghai in order to serve a London client. In a case like this, the professional staff expects the performance of key applications will be the same regardless of where the application is located.

In a collaborative work environment, sharing files and information over the corporate network becomes a critical

communication path. Attorneys spend a significant amount of time accessing research, client information and historical data stored throughout the company. When attorneys cannot access the information efficiently, they must work harder to give the client the level of service they deserve. Most organizations have recognized that the WAN has the potential to enable seamless, productive communication among offices but haven't been able to achieve the level of WAN performance necessary to make this ideal a reality.

Enabling better interoffice client teams via the WAN consists of two critical components: faster information access and centralized information, both of which depend on higher WAN performance. That's where the WAN optimization power of wide-area data services (WDS) comes into play.

Understanding Wide-Area Data Services

Before WDS, most law firms and law departments could only hope to accelerate the transfer of a few distinct types of data across the WAN. One approach, called file caching or wide area file services (WAFS), helped improve file sharing. But caching is limited in scope and requires significant amounts of remote infrastructure management. It was a good step toward a solution but not the end goal, because files are only one form of data used by attorneys. Another potential alternative, network compression appliances, reduced the amount of information moving over the network, but they did very little to reduce redundant data transfers or deal with latency.

Early in 2005, the analyst firm Taneja Group noted that a set of vendors were creating products that took a broader, holistic approach to solving the problem of poor network performance. The approach aimed to combine the power of WAFS with network compression and application acceleration. The Taneja group declared, "Wide-area Data Services (WDS) is about much more than file services across the WAN; it encompasses TCP optimization, data reduction for replication, e-mail caching and a range of application protocol optimizations" (*Wide Area Data Services: Optimizing the Branch*, May 2005, The Taneja Group).

The impact of WDS technology can reach across all IT responsibilities. In the same paper quoted above, the Taneja group laid out some of the impact of WDS on the organization:

Centralizing distributed infrastructure like file servers, mail servers, Network Attached Storage (NAS) and remote office backup systems — without affecting remote users

Sharing large files among colleagues on different continents — as if they were in the same building

Performing backup and replication over long distance WAN links — and completing them during small backup windows

Delivering significantly more services on existing WANs — without upgrading bandwidth

Technologies built on the WDS concept take a holistic approach to optimizing WANs, performing optimization activities across all applications. At the same time, these products are designed with the ability to plug in additional optimizations that are specific to certain protocols. For example, common inefficient protocols such as CIFS for Windows servers, MAPI for Microsoft Outlook or MS-SQL for database applications can get special help from WDS products. Customers typically see application performance improvement that ranges from five to 100 times faster than unoptimized performance and bandwidth reduction that ranges anywhere from 60 to 95 percent. The actual improvement will vary by customer based on the applications used and network characteristics.

WDS products are deployed on each end of a WAN connection, with one-to-many connectivity for a centralized device. WDS focuses on the three main problems in WANs: bandwidth limitations, TCP protocol inefficiency and application protocol inefficiency. These problems are addressed in different but complementary ways.

Bandwidth limitations are handled by taking as many bytes out of all types of data transfers as possible and optimizing the way the rest of the bytes are sent across the network. WDS technologies either compress data or take bytes “off the wire.” Compression is well understood, but the concept of eliminating data transfers deserves a detailed look.

The best WDS products break up files and data into small segments in an application-independent way and store them in memory or preferably on disk. Then, any time data tries to move across a WAN link, the devices look on a disk or in memory for repetitions across all applications to see if the bytes have been previously sent across the network by any other application. For bytes that have been sent before, the server-side device sends small references across the network instead of the actual bytes, typically saving 65 to 95 percent of data from transfers.

Bytes that are new are compressed, sent across the network and then stored on the client-side device for comparison against future transfers. Using a combination of references

and new data, the client-side device reconstructs the file and delivers it to the user. This method of storing bytes and checking for redundancy should ideally be implemented as a bi-directional service, meaning that if a user in a remote office downloads a file and then later uploads a modified version of the file, the WDS devices will recognize that the bulk of the bytes are redundant. Disk-based devices perform better because they have a larger data store against which to compare requested bytes.

For example, consider two attorneys collaborating on a contract across the network. The first attorney writes the contract and e-mails it to another attorney across the country. Since the contract is totally new, the WDS appliances compress the information and send it across the network, saving some bandwidth. The second attorney makes some changes, modifies the file name and posts it to a document management system based in the same office as the first attorney. This time, since the WDS appliances have seen the data, only the bytes that have changed in the second attorney’s version are sent across the network. This happens even though the attorney changed the file name and is using the document management system instead of e-mail. Therein lies the power of WDS — by working across all applications and examining data on the byte level, the technology can provide massive bandwidth reduction for all data.

Further Considerations

To take full advantage of available network capabilities, IT managers must address more than just bandwidth. Latency is a secret throughput killer on the WAN, especially when poorly behaved application protocols add overhead beyond TCP’s overhead. TCP as well as application protocols suffer from a problem called chattiness. In order to ensure reliable transport in sometimes unreliable environments, these protocols were designed to send very small amounts of data (16 to 64KB) and then wait for an acknowledgement from the receiver. Given that latency adds milliseconds to each trip of a packet across the network, the process of sending a file that is possibly multiple megabytes may take minutes upon minutes.

The best WDS technologies approach this problem by addressing TCP directly for all applications that run over the network, and also creating a platform that allows for plug-ins to address the quirks and inefficiencies of application protocols. Others are trying to partner with network compression vendors in an effort to match the performance gains of more complete WDS products. The most popular protocols are already often addressed, including CIFS for Windows servers, MAPI for Microsoft Exchange, HTTP and FTP. The most advanced products are aggressively adding other key protocols to their devices, such as MS-SQL.

Meeting the challenge of latency while maintaining the reliable nature of protocols is where WDS products really shine. While TCP may have trouble overcoming latency, it is a very “safe” protocol that will handle congested or “lossy” networks. WDS products aim to maintain the safe nature of the protocol while optimizing data flow. TCP optimizations in WDS products often include adaptive window scaling to send more information in each packet, faster packet loss detection, selective and delayed acknowledgements, and congestion window validation for bursty applications. Ideally, the product has implemented these features in compliance with IETF (Internet Engineering Task Force) standards. The most powerful impact of TCP optimization occurs in conjunction with how the WDS device handles bandwidth reduction. If the product eliminates data and sends references instead of actual data, then each TCP window can be packed with references. Each reference can point to an almost unlimited amount of data, essentially “scaling” the TCP packet from 64KB into hundreds or thousands of kilobytes. This functionality can eliminate a staggering 60 to 98 percent of the round trips needed to complete a file transfer, minimizing the effects of latency while maintaining the “safe” nature of TCP transmissions.

Application protocols are handled in a similar way by reducing the number of round trips generated by the application (separate from those required by TCP), but the actual optimizations vary for each protocol, its quirks and where it has significant inefficiencies. If the WDS product is designed from the ground up to handle all TCP-based applications, it will almost always provide performance improvements to the application even if it does not have an application protocol-specific module. However, if the application’s throughput is limited by the way the application itself works, then fixing TCP alone won’t solve the problem. With an application protocol-specific module, improvements delivered by optimizing bandwidth and TCP can be increased by a large multiple. By understanding the application protocol (such as HTTP, CIFS or MAPI), the WDS device can do the “heavy lifting” of file access or file saves on the LAN and then only send the optimized data over the WAN.

Benefits Across the Organization

WDS products are a type of IT infrastructure. They transparently facilitate the flow of information. While they are not visible to the organization in the same way that new applications are, WDS products will nonetheless affect all key stakeholders that use the WAN.

Attorneys and staff see dramatic changes in the performance of applications and transfers over the WAN. And the WAN is less of an impediment to the practice of law, eliminating frustrating, non-billable tasks that require everyone to spend

more time doing back-office activities that do not directly benefit the client or simply take more time than they should. The speed of activities such as collaborating on a contract or discovery does not need to be limited by the amount of time to send information back and forth.

In addition, IT managers will see a number of benefits to their internal operations and workflows. First, IT applications such as remote WAN backup and upgrade management will be accelerated dramatically, just as user applications are. More importantly, the performance enhancement of user applications means that applications and infrastructure can be centralized. File servers, backup equipment, applications and other tools that are difficult and expensive to deploy and manage remotely can be consolidated into the corporate data center with no degradation of performance. IT managers can eliminate significant hardware costs, simplify infrastructure deployment and management and focus their staff on forward looking IT projects instead of fire-fighting, fielding user complaints and manual maintenance.

Finally, partners of the organization will recognize this type of solution as good for business. Providing better client service will assist in maintaining good client relations, and eliminating non-billable tasks that impede attorney practice will create a better environment for everyone in the organization. And of course, the tangible cost savings behind consolidating IT infrastructure will be of interest to anyone who wants to make the company more successful.

In Practice: Allen Matkins Case Study

While understanding the mechanics of a technology is important, the true test is seeing how the technology fares in a real-world environment. Allen Matkins Leck Gamble & Mallory LLP has deployed WDS technology that has dramatically changed the way the firm does business. With more than 200 lawyers located in five major business centers in California, their practice is national and international in scope. The firm has developed 17 highly successful practice areas including Corporate and Securities, Litigation, Real Estate, and Technology.

The key driver for Frank Gillman, Director of IT at Allen Matkins, was to optimize the existing network infrastructure to support the way their attorneys collaborate across offices and across practice groups. Critical applications for Allen Matkins include Interaction CRM by LexisNexis and DOCS Open document management by Hummingbird.

Gillman and his team deployed one WDS appliance in each office. “We had considered adding more bandwidth and hardware, but the annual leasing expenditures made a bandwidth upgrade prohibitive.”

Auto-Capture Time on the Phone

by Ray Deck of Element 55

WDS technology has enabled the firm's attorneys to focus on delivering the best possible client experience without enduring frustrating downtime, lost hours and nonbillable overhead. Gillman estimated, "With our WDS solution, we have eliminated more than 20 nonbillable hours annually for the average attorney working in a remote office. Now we can provide our high-quality client experience while eliminating behind-the-scenes manual labor by our attorneys. That also translates into an estimated \$980,000 in annual productivity gains for Allen Matkins.

"Litigation case files, which took more than 22 minutes to download, can now be downloaded in two and a half minutes for a cold transfer. Edits followed by a transfer across the network take about eight seconds. No amount of added bandwidth could do that for us."

WDS products have also enabled consolidation of IT infrastructure. Because access to information is now accelerated, critical client data and documentation can be stored centrally, where all practices can access it. "Because of WDS, we no longer need to maintain as much remote IT infrastructure. We have changed the way we deploy remote infrastructure and backup remote data, for the better," concluded Gillman.

Summary

Law firms and law departments will find that WDS technology has a positive impact in a number of areas across their organizations, most importantly enabling attorneys to provide better client service while eliminating frustrating nonbillable tasks. IT managers can make the WAN more effective, reducing user complaints as well as simplifying standard IT tasks. Infrastructure consolidation is also feasible, as the Allen Matkins case study shows.

WDS technology complements existing IT infrastructure in firms and law departments that share information, data and files among offices. WDS vendors implement solutions from slightly different perspectives, but overall the technology provides a significant boost in network performance by attacking the root causes of network limitations.

Mainstream law firms and law departments that are local, national and even global in scope have rigorously tested and deployed WDS technology. Any organization that has a wide area network should consider WDS technology as an ally in the pursuit of optimum WAN performance.

A large part of an attorney's day is spent on the telephone — with colleagues, clients, court and opposing counsel. Much of this time is billable — but not all of it gets billed. The systems that manage phone calls provide an opportunity to capture the time without having to remember when the call started or manage a stopwatch. Automatically capturing time spent on the phone is possible, and it measurably improves the completeness of time sheets and firm revenues.

Research indicates that time related to phone calls is one of the most difficult to recall because of the sheer volume of calls and the uncertainty of their length. Attorneys spend time at the end of the week or month staring at their time sheets trying to remember, "What calls did I take from this client?"

Capturing Phone Time

All office phone systems can generate call detail records (CDR) or station message detail records (SMDR) with the following information:

Which extension made/received the call?

Was it incoming or outgoing? (Or, in some cases, extension-to-extension)

When did the call start?

How long was the call?

With whom was the call? (Phone numbers are always available for outbound calls and inbound calls with caller ID.)

Chances are your organization captures at least some of this information already. Cost accounting systems associate outbound minutes with particular clients to allocate disbursements related to the phone bill. If you have to dial an account code to make a long-distance call, you definitely have one of these. But traditional cost accounting is about capturing the pennies per minute on outbound calls. With automatic time capture, you have the opportunity to capture the hundreds of dollars-per-hour attorney time associated with all phone calls.

Feeding the Time Sheet

The key to realizing this opportunity is getting the time from the phone system to the attorney's time sheet. The more automated the process, the easier it is to capture more time, and the attorney spends less time trying to remember a given call.

Capturing phone time for the time sheet has different requirements than cost recovery:

Update in Real Time

Attorneys expect to see information about what they've done within a few minutes of hanging up the phone. In contrast, cost recovery processes can only queue up information and process it at month end when bills go out. To contribute to the time sheet, the processing of phone-related information must be accelerated to be available to attorneys in a much shorter timeframe.

Capture All Calls

While cost accounting looks only at outbound calls for disbursement purposes, attorneys spend even more time on inbound and internal (extension-to-extension) calls. While the phone system may not be initially configured to generate this wider output, it can be, and capturing these additional calls dramatically increases the value for attorneys.

Integrate with CRM

Customer relationship management databases (*e.g.*, InterAction, Outlook, Notes) let you convert a cryptic phone number into a useful name and company that the individual called. There is an enormous difference in usefulness between: "Phone call to 912125551234" and "Phone call to John Smith (ABC, Inc.)." The prospect of descriptive phone-related time entries also incentivizes the use of CRM, creating a virtuous cycle.

Put It in Context

Phone calls do not happen in a vacuum — e-mail messages, document preparation and other activities are often part of the preparation or follow-up related to the call. Presenting activities done before and after the call lets the attorney allocate all the time, rather than just the portion actually on the phone.

Make the Connection

The technical requirements for capturing phone time data to the time sheet will vary based on the models and systems involved, but the process involves five steps:

Configure the Phone System

While all phone systems have CDR features, they are not always turned on unless a call accounting system is already attached. Even after confirming that CDR is active, make sure

that all calls are generating records — local outbound, inbound and, if possible, extension-to-extension calls. Also, including caller ID (often called ANIS) in the record adds a great deal of value to the captured inbound calls. This configuration is a matter of changing a few flags in the software.

Extract the CDR Stream

In older phone systems, CDR is streamed over a serial connection that can be tapped with a terminal program or serial logger. In newer systems, the data can be captured using a network service. If there is already a call accounting system in place, the time capture system should share the feed.

Parse the Records

Once the record is captured, the key data points need to be extracted. Each phone system vendor (and sometimes each model) has a different way of laying out the CDR.

Process through CRM

Match the phone number in question with an appropriate contact whenever possible. Contact management systems have different mechanisms available for extracting this information.

Add to the Time Sheet

Finally, with all the data points in hand, the newly minted time entry should be pushed to the automatically generated time sheet, where it can be used as a reference or revised and submitted to accounting.

An integrated automatic time capture system will take care of these five issues at one time, as well as put the phone calls in a rich context of other activities, such as reading e-mail, revising documents and attending meetings, all captured without the attorney ever starting or stopping a clock.

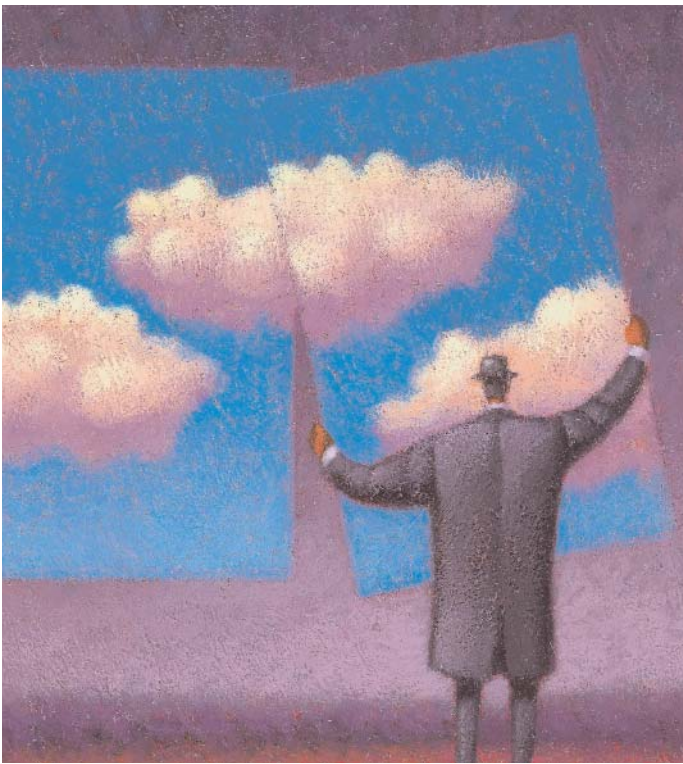
What's Next? Capture More Billable Hours

Cell phones, BlackBerry devices and other communication devices represent an additional opportunity to capture communications. Further, once attorneys have a taste of automatic time capture from one system, they'll ask, "Why not for everything?"

Automatic time capture is an opportunity to increase the completeness of time sheets and leverage your existing (phone, customer relationship) technology investments. For a relatively small cost — and without requiring additional work from attorneys — the firm or law department can reap the benefits of capturing more billable hours.

Creating Omnipresence Through Video Technology

by Jack M. Sheekey of VideoTeleCon



Although videoconferencing and video streaming have been around for years, the technologies were typically not available except to those with deep pockets and a tolerance for technical complexity. However, over the past few years a confluence of events has rapidly driven the adoption of these technologies as a viable alternative to travel.

These factors include globalization, the ubiquity of broadband, terrorism and the increasing difficulty of air travel. Along with the increased value of face-to-face communication in an Internet-based economy, the trend has driven every level of the profession to integrate video technologies into the practice of law.

Videoconferencing

Until recently, firms and law departments have primarily used videoconferencing for internal management, administrative communication between offices and interviewing job candidates. Videoconferencing has also been used to reduce international travel, confer with clients or as a “backup” to

travel when scheduling changes or transportation issues become unavoidable.

As costs have lowered and quality continues to improve, even attorneys in smaller firms have begun to integrate videoconferencing into their practice. It is now common for attorneys to use videoconferencing to depose witnesses, consult with experts, co-counsel and clients and even run settlement conferences and mediations remotely, especially when multiple, far-flung parties need to come together on short notice.

The spread of videoconferencing throughout the legal profession has not been limited exclusively to law firms and law departments. Many courtrooms, bar associations, arbitration and mediation companies, trial consultants and expert witnesses have installed it at their locations to enable spur-of-the-moment, face-to-face meetings with counsel and clients. For those who don’t yet have videoconferencing in their own office, a booming trade has developed, particularly among court reporting firms, to provide videoconferencing “public rooms” on an hourly or daily rental basis.

Video Streaming

Within the legal profession, video streaming has been used primarily for CLE and other practice development and training applications. A limited number of progressive attorneys have also used video streaming to deliver remote depositions to colleagues, consultants or clients. When remote “real-time” depositions are desired, the majority of attorneys have streamed only text due to the bandwidth requirements and complexity of sending both the audio and video. In some extreme cases, attorneys have even brought in satellite trucks to beam proceedings from remote areas or courtrooms. Thankfully, the logistics and expense of this approach are no longer necessary.

The ubiquity of high-speed Internet connections combined with improved video compression and inexpensive hardware has created an explosion of video on the Internet. In the legal profession, this has prompted attorneys to extend the use of video streaming far beyond its initial use as a way to deliver education-related content.

Attorneys are now streaming depositions, mock trials, expert witness consultations and even court proceedings to remote parties. In short, attorneys are using video streaming for all of the same applications for which they use videoconferencing.

The only difference is video streaming is used to broadcast a one-way stream to “passive” viewers instead of enabling two-way communication between two or more parties via a videoconference.

How Does This Technology Benefit the Firm?

When streaming first gained prominence on the Web, the big “events” were live concerts and other high-profile “webcasts.” The archives of these events were often treated as afterthoughts. What quickly became apparent was more viewers watched these events after, rather than during the live event.

The ability to watch what you want, WHEN you want quickly became one of the primary benefits of the technology. This phenomenon, known as “time shifting” is now an expected feature in “content delivery.” Whether it’s a CLE seminar streamed to a desktop, a TV show caught on TiVo or a radio program downloaded to an iPod, the world is rapidly moving toward an “on demand” model.

The impact of time shifting on the practice of law is no less revolutionary. For attorneys, whose primary resource is time, this ability to shift time and space via video is creating a dramatically different work process and lifestyle.

Any meeting that takes place in a videoconference can automatically be recorded using a DVR or even an old-fashioned VCR. No additional administrative or technical help is required beyond hitting the VCR’s record button at the start of the meeting. No attendant or videographer is required. In fact, videoconferencing equipment is often used expressly for the purpose of recording on-site meetings and video “memos” to others. The simple user interface (a remote control) is something most attorneys can use without needing administrative or technical assistance. Once they have a recording, it can be shared with co-counsel, clients, trial consultants and others.

Recorded meetings can also be digitally encoded into mpeg files and dropped into popular trial presentation software packages. Encoded video can also be streamed live or from an archive.

Greater Participation

Instead of sharing text transcripts, attorneys can now share video depositions and other meetings with partners, associates, paralegals, trial consultants, co-counsel, experts and clients. This brings up another benefit to the firm — greater participation.

By shifting time and making meetings available to anyone with a VCR or Internet connection, everyone involved can literally see what’s happening from their desk, home or hotel

room. The ability to include senior partners in depositions to which they wouldn’t normally travel adds tremendous value to the work product of the associate who captures the deposition.

Conversely, a senior partner can question a witness and have a team of associates, trial consultants and paralegals participate from remote locations. Those who need to interact can participate by videoconference. Those watching “passively” can do so from their computers. However, the passive participants can marginally interact by instant message with the questioning attorney or each other. For those who can’t participate live, there’s always a copy in the archive to review later.

Client Relations

Client relations are greatly improved when attorneys communicate and share their progress with clients. Keeping in mind that the “client” may not be a single person but a corporate legal department that interacts with a firm on many levels, you can see how the benefits of these technologies can improve relations. Clients who have face-to-face access to attorneys, trial consultants and experts — even from an archive — will be better informed about a case’s progress.

Attorneys who include clients at key events leading to trial, such as choosing an expert witness or viewing a mock trial, greatly increase clients’ understanding of the process and comfort level. This builds trust and makes it easier for attorneys to justify strategies, expenses and ultimately aids client retention.

Cost Savings

Cost savings (attorneys billing from their desks instead of an airport) are self-evident. Granted, plaintiff attorneys who are spending their own money may be more focused on expenses than some defense firms, but ultimately the cost savings and efficiency is a boon to all. According to a Washington Post story, Akin, Gump, Strauss, Hauer & Feld, L.L.P. “saved the firm hundreds of thousands of dollars for airline tickets, hotel stays and car rentals, and it has cut the unproductive hours spent in airports.” In less than a year of videoconferencing, the firm “cut its travel spending by 60 percent, or about \$250,000.”

During a recent trial involving a large entertainment company, an army of attorneys from both coasts watched a live video stream of the trial from their offices. Attorneys and staff were able to watch testimony, receive a real-time transcript and review exhibits as they were presented in court. Both plaintiff and defense firms were able to privately pass research, trial exhibits and messages back and forth to their respective trial teams in the courtroom. Imagine what it would have cost to set up separate war rooms in Delaware and feed, house and

shuttle people back and forth to both coasts during this three-month trial.

The ability of these technologies to shift time and space, increase participation and lower travel costs has tremendous benefits for the firm. As attorneys utilize these technologies to interact more with their clients, the professional relationships between them will deepen and become more beneficial to both parties. In addition, the benefits to attorneys are having a dramatic impact not only on their professional lives but their personal lives as well.

Common and Creative Applications

The “bread and butter” application of these technologies in the litigation process is capturing and sharing depositions. Attorneys usually “discover” videoconferencing when they need to be in two places at once or when their travel plans fall apart.

Depositions

The ability to depose a witness across the country from your own conference room or even a rented “public room” down the block makes tremendous sense. Why fly when you can place witnesses in a public room and interact with them face-to-face? There are now over 4,000 public rooms available for rent worldwide with over 300 court reporting firms hosting videoconferences in the U.S alone. Medical centers, universities and shared office facilities typically offer videoconferencing facilities.

Streaming the deposition (from a videoconference or not) to passive observers increases flexibility and reduces costs even further. Any time an attorney is considering doing an “Internet dep” (streaming text in real time to remote parties), a video stream can greatly enhance the experience. Body language, demeanor and overall credibility can play a crucial role in how a witness’s deposition will be handled. Also, the ability to watch opposing counsel ensures that the witness is not being “coached,” something that can’t be determined by using only a phone or text feed.

Using Experts

Some attorneys are becoming very creative in how they use videoconferencing to hire and work with expert witnesses. Initial consultations with experts can have the following benefits:

“Prescreening” the expert. Being on camera is similar to being on the stand and can be a great preview of how the expert will perform in court.

Selling the expert. Reputable experts are busy and may not have time to take every case because of

scheduling conflicts. Knowing that they can work with you by videoconference may increase their availability by minimizing travel time.

Selling the client. Recording an initial consultation and sharing it with the client can get them to sign off on using a more appropriate expert than is available locally. Emphasizing their unique expertise, along with the fact neither party will need to travel to prepare for trial will help with the buy in (especially when they’re paying for travel and the expert’s time).

As trial preparation begins, the freedom to call quick meetings on short notice enhances the team’s ability to move forward without having to coordinate less frequent, longer meetings. Streaming depositions of key witnesses to your expert can also provide valuable real-time feedback to the questioning attorney. The expert can “pass notes” electronically to the attorney to guide the questioning or highlight technical inconsistencies in the testimony.

Use in Court

Use of videoconferencing and video streaming in the courtroom is becoming much more common. Witnesses who can’t travel are appearing by videoconference, proceedings are being streamed back to offices and war rooms, and even video arraignments between courts and jails are becoming more common.

Many courts now have videoconferencing available onsite. Others will allow temporary connections to be installed. Most will not allow you to tap into their own network, but the installation of lines on a temporary basis is fairly straightforward with vendors specializing in this service. To stream video, an encoding box is simply connected to a camera and uploads the file to any broadband connection.

Underlying Technology and Options

Streaming — The ability to move audio and video across the network depends on a number of underlying technologies. The most familiar is the file itself, most commonly a Windows Media File (“wmv”). Since Microsoft makes their media player an integral part of the operating system, Windows Media Player and files have become ubiquitous. Although other formats and players have their unique features for the purposes of encoding and playing video, the wmv has become the *de facto* standard much like the MS Word “doc” is for text.

The first step in the process is encoding the file. A software codec (compression algorithm) is employed to convert media into a wmv. Transmission of the encoded file to a “streaming server” requires a constant connection of ~256k to transmit a

good quality file which will display a viewable image of roughly 3 by 4 inches. The streaming server is simply a computer that runs software to push streams out at the request of a user. To deliver streams across the Internet with any degree of consistency, an “edge network” of servers located near the recipient is employed. These servers are connected by a dedicated IP network engineered specifically for video. The servers themselves are also configured for this purpose with each serving as a “mirror” to distribute the file intact to end users, without interruption from network congestion.

Replication of this solution from end to end is arduous and expensive. Fortunately service providers serving all or part of the food chain make it easy to do. Hardware companies sell encoding devices, ISPs provide streaming servers, and other service providers offer edge networks on a temporary or permanent basis. In the legal market, many court reporting firms provide an end-to-end solution from their office suites or can refer you to service providers who can provide streaming from your office or a remote location such as a courtroom or war room.

Videoconferencing — Videoconferencing takes streaming one step further. The ability of all parties to communicate back and forth introduces a level of complexity and greater bandwidth requirements, but it includes the same components: a hardware device with codec, a specially engineered network and a “player” at the other end to decode the signal. In this case, however, the devices on each end serve as both encoder and decoder (player).

Videoconferencing systems attach to TVs or Plasma/LCD monitors via S-Video or VGA connections. They are self-contained and do not need to be connected to a computer. Additional peripherals such as VCRs, DVDs, document cameras (“ELMOS”), projectors and laptops may be connected to display exhibits of all types to either side.

Videoconferencing systems used for “internal” purposes between offices may be connected over IP across a Multiprotocol Label Switching (MPLS) network that insures a level of Quality of Service (QoS). Videoconferencing over IP generally does not match the quality of connecting over ISDN phone lines. ISDN at 384k (three lines) is the standard for connecting between public rooms. Any “external” connections to rooms not on the same MPLS network should go over ISDN to insure greater QoS. ISDN has the added benefit of being as secure as a regular phone call, because you are dialing point-to-point rather than going through the Internet.

384k is required to provide 30 fps video (broadcast quality) and full duplex audio (no “clipping” of voices if two or more are speaking simultaneously). When running at “384” over IP, you will need to provide ~500k in dedicated bandwidth on each side to account for “overhead” and variations in the connection. Connecting between ISDN and IP rooms requires a gateway service, usually provided by your bandwidth supplier at additional cost. Bridging multiple sites for multipoint calls also requires an outside service provider. Although it is possible to bridge your own multipoint calls with an internal bridge, you need to be sure to have enough bandwidth. Each site in the call will require another 384k (500k if IP) at the host site. Unless there’s a defined application to bridge calls on a regular basis between fixed offices (with a clear ROI), it is not recommended to buy your own bridge and host this internally.

The Future

The future of videoconferencing and streaming is now. Attorneys are rapidly adopting these technologies to their practices much as e-mail and the Internet took off in the mid-90s. Essentially, these technologies are just the natural progression of the Internet revolution. With ubiquitous, low-cost bandwidth and video players on every desktop, it’s only natural for video files to share the network along with the millions of documents sent by e-mail every day.



Understanding Your Wireless Needs

by Berylle Reynolds of MBR Wireless Consulting

There are about two billion wireless users worldwide (estimated by Wireless Intelligent, a venture between Ovum and the GSM Association). According to the U.S. government, cell phones have outnumbered traditional land-based phone lines in July of this year. It comes as no surprise that many businesses, including law firms and law departments, are including wireless as part of their business tool set. Some companies have even gone as far as discarding their land-based phones and gone completely wireless.

Wireless was introduced into the legal environment (and businesses) almost haphazardly. It started with one or two partners wanting a wireless phone to communicate with their clients while in transit. Pretty soon it spread to every lawyer, IT personnel and other support staff. However, increases in usage led to increases in cost, and confusion was setting in with carriers continually changing the pricing structures, technologies and their support representatives. Eventually, the organization needed someone to communicate with the wireless carriers to handle these issues, and the assignment went to someone who seemed to be good at it. It might have been an administrative assistance, a telecom manager or some random soul from the IT department. However, what was thought to be a small task suddenly became a full-time job. This sudden “wireless manager” gradually became the wireless expert for the organization. In addition to spending time on the phone with the carriers, he or she also had to answer questions from the wireless users.

Wireless should make life easier for companies, not add burdens and frustrations. When properly managed, the benefits wireless provides are tremendous. Wireless lowers the cost of conducting business while allowing users to be more effective. To assist you in effectively managing your wireless program, we will explore various issues a wireless administrator should consider. We coined the phrase “wireless management” to describe managing any aspect of an organization’s wireless-related issues.

Even though “wireless” can refer to a wide-range of technologies, including telegraph, two-way radio, Wi-Fi,

Wi-Max, BlueTooth and cellular, we’ll refer to “wireless” as cellular services offered by carriers such as Cingular, Sprint and Verizon.

Assessing Wireless Needs

Overspending is costly, so is underspending. A firm or law department wastes money when providing wireless to an employee who does not need it. Yet, it is equally costly when an organization does NOT provide wireless to someone who needs the technology. To understand what you actually need, you must begin with a detailed assessment. This evaluation provides a guideline to how many wireless handsets are needed, what types of technologies should be in place and the budget for wireless needed for the next few years.

Begin with assessing your current wireless needs. Some steps in gathering information during the assessment include:

Count and group personnel based on their wireless needs.

Determine locations because a carrier may serve one location very well but does not have adequate coverage in another location.

Take inventory of current wireless devices.

Rank each group’s needs for wireless telephones. Employees who need just a wireless phone are those who are often out of the office, and it is critical for others to reach them.

Rank each group’s needs for wireless data devices. A wireless data device would be useful to employees who need to access applications and check e-mail while they are out of the office.

Armed with the necessary data, the organization can now deploy wireless to those who need it most. If the budget allows, it can then be deployed to the next groups. If the organization plans to arm everyone in a critical location with a wireless device for use in an emergency, wireless carriers offer ways to provide these devices at a minimal cost.

Issues to Consider

With a clearer picture of the organization’s needs, there are a few more factors you must consider to properly assemble the right wireless program.

Future Expansion — Consider the organization’s plan for expansion. Estimate how many new employees and locations are being added. Will there be international growth? This information will be useful in choosing the right technologies.

Disaster Recovery Plan — If the organization has a disaster recovery plan in place, find out whether wireless is part of the plan. During the anthrax incidents that followed 9/11, some post offices deployed wireless data devices to immediately notify employees to clear the facility if anthrax was detected. Employees could then respond when they had evacuated. Many firms today have added wireless to their recovery plans to allow them to be up and running more quickly and easily at an alternate location. Of course, even wireless cannot guarantee 100 percent availability during disasters (witness Hurricane Katrina), but it is often the first communication network to be restored right after a disaster hit.

How Much Technology to Provide

The average monthly cost for a wireless voice plan for business users is about \$50, and the cost of a wireless e-mail service can add another \$50 to the monthly invoices. This cost does not include the initial equipment investment such as the price of handsets and wireless data servers. Sometimes the benefits of wireless services cannot be justified by dollar savings alone. No one can put a price tag on an attorney's ability to check e-mail while waiting for his/her flight in an airport. So how much technology should be provided?

An organization can provide employees with voice, data or both. Providing data allows users to check e-mail or input billable time while away. One firm found that after each attorney had a wireless data device to input billable time, the total billing increased 25 percent in the first three months, which completely paid for the devices and service for a year. If a firm provides only a cell phone, users cannot take advantage of wireless data.

Cellular Technology: CDMA vs. GSM

Determining the right wireless technologies to deploy can be tricky. In the U.S. alone there are two main competing cellular technologies: CDMA and GSM. (Just two years ago, there was a third technology called "TDMA," but it is not widely used in the U.S.) Each technology has its own branches of technologies. Within GSM are EDGE, GPRS, WCDMA, UMTS and HSDPA, and within CDMA are 1XRTT, EVDO and EVDV. Cingular and T-Mobile use GSM, while Verizon and Sprint use CDMA. Some time ago people speculated that these two branches would eventually unite as they advanced into 3G, but currently, they are still separate.

The organization should carefully consider which technology and devices to use, because once deployed it can be costly to switch. The cost of handsets, termination fees, deployment time and disturbance to employees can be high when switching from one technology/device/carrier to another. If,

after careful evaluation, you determine you need a different technology, further considerations are necessary. Will the benefits of switching to a new technology outweigh the switching cost? What is the ROI?

Which is right for you, GSM or CDMA? According to Wireless Intelligent, the GSM family of technologies currently has 78 percent of the world market. This is because GSM is used worldwide while CDMA is primarily used in the U.S. However, it does not mean that GSM is better than CDMA. CDMA offers better data speed and better coverage in certain areas. Next generation CDMA technology is usually backward compatible with the older CDMA network, allowing users to keep their old devices even as new CDMA technology is rolled out. However, when a new GSM technology replaces an old GSM technology, the old GSM devices are rendered useless. Since both technologies have their pros and cons, you must consider coverage, data speed, handset selections and pricing to determine which is right for you. Some organizations adapt both technologies and deploy them depending on the location. For example, let's take a firm that has locations in New York, California and London. Users in New York frequently travel to London while their California counterparts typically stay in California. The location in New York may use GSM devices because it allows their users to use the same phones when in London, while the users in California may have CDMA due to coverage.

Choosing Wireless Devices

Aside from cellular technologies, the organization must also consider whether to deploy wireless voice-only devices and/or wireless data devices. The diversity of devices available today makes the decision difficult. Furthermore, the latest and greatest device today may become tomorrow's paperweight. Bear in mind that a device purchased from one carrier cannot be used with another, even if the carriers use the same cellular technology.

Cellular Phones — With so many different cell phones on the market, you should set rules as to which devices to deploy. Allowing users to choose what they want may increase the users' satisfactions on the devices, but it could be a nightmare to track these devices and arrange for replacements if they become lost or stolen. Although some cell phones allow users to check and respond to e-mail or surf the Web, these functions are limited due to the size of the phones and the associated numbered keypad. Accessing data on a cell phone may be costly, because fees are typically based on how many kilobytes are downloaded. Set policy and place restrictions as to how users access data on their phones.

Wireless Data Devices — Wireless data devices include wireless laptop cards and wireless e-mail devices. Wireless laptop cards are PCMCIA cards that allow users to connect their laptops to the cellular network to access the Internet. Wireless e-mail devices allow users to check e-mail and access certain corporate applications all from a small handheld device. Yet, because their keyboards and screens are so small, they cannot completely replace laptops. Many of today's wireless e-mail devices also allow voice calls, allowing users to carry one device for both voice and data.

Wireless Enterprise Servers — To deploy wireless e-mail devices, an organization should install an enterprise-grade wireless server to ensure data exchanged between the corporate server and the wireless devices is secure. The enterprise-grade server software is referred to as the wireless enterprise server, while the software residing on the handheld device is referred to as the client. Several companies, such as BlackBerry (RIM), Goodlink (Good Technology), SEVEN and Visto offer wireless enterprise server/client software.

There are two ways wireless enterprise servers send data to the end users: "push" or "pull." A server pushes e-mail to the user's device whenever a new e-mail arrives at the server. In the "pull" scenario, a user needs to manually check the server to see if new e-mail messages have arrived.

A wireless enterprise server can be installed behind a firewall or through a firewall. In the behind-the-firewall scenario, the wireless enterprise server is connected directly to the corporate e-mail server and sits behind the firewall. When a new e-mail arrives, the wireless enterprise server will either push it directly to the user's device, or provide it to the user when he or she pulls for new e-mail. The organization must provide the hardware for the server software to reside. This option is more costly than the through-the-firewall option, because the law firm or law department needs to pay for equipment, software and maintenance. However, most organizations opt for this because they have more control over the data. Many people also feel, erroneously, that through-the-firewall is less secure.

In the through-the-firewall scenario, the wireless carrier hosts the server. A VPN or SSL connection is necessary to connect the server on the carrier side, through the corporate firewall and to the corporate e-mail server. The entire link is secure. SEVEN (www.seven.com), which provides this option via Sprint/Nextel and Cingular, claims that no e-mail messages are stored on the carrier's side. All e-mail messages are simply forwarded to the users. This option is much cheaper, as no equipment, software or maintenance are required.

When selecting the right enterprise server platform, you must consider handsets, ease of deployment and available support.

For example, BlackBerry is the most common server/client platform used today. However, since BlackBerry is proprietary software, it can only be used by devices made by RIM. (This may change as RIM is planning to license the BlackBerry client to other device makers.) Good, SEVEN and Visto can be used on any devices.

Choosing the Right Carrier

Because carriers usually demand an initial two-year contract, switching carriers during the contract term can result in large termination fees and expensive new equipment. It also takes great effort to coordinate porting mobile numbers from one carrier to another and distribute new phones. Therefore, it makes sense to pick the right carrier(s) from the start, in order to prevent any costly switch later on.

Coverage — An organization that has several locations, either in the U.S. or around the globe, should consider the carrier's coverage for each location. Putting other factors aside, GSM may be the better choice if your organization has worldwide locations and users travel to these locations consistently. However, there may be cases that GSM coverage is lacking in domestic locations or higher CDMA speed is desired. In these cases, one must weigh the convenience of traveling with the same phone and number for both U.S. and international, or gaining better coverage domestically and rent a world phone when overseas. Fortunately, GSM coverage in the U.S. is improving, and GSM broadband technology is gaining speed.

Data Roll-Out Plan — Two carriers who offer the same cellular technology, CDMA or GSM, are not alike when rolling out their broadband strategy. Implementing broadband is very costly for carriers. Each new technology requires new equipment and software to be installed at the cellular site. And today's fad may become tomorrow's old news. If the carrier made the wrong bet, millions and even billions of dollars can go to waste. Therefore, one carrier may become reluctant to roll out the next-generation technology while another may charge ahead. When selecting a carrier, you should look at whether the carrier's data roll-out plan will meet your requirements in the near future.

Support — Each carrier manages its sales force and support teams differently. Some carriers have decentralized sales and support teams, offering an organization a different team for each location. This decentralized approach has some downsides: You will receive multiple invoices (except with e-bill, but more on that later), and you will have multiple places for purchasing. Carriers that have centralized sales and support teams provide organizations with a single stop for support and purchasing. Customers who require local support should request that before signing the contract. Carriers also offer business discounts based on the number of lines the

organization owns. Carriers with decentralized teams may base the discount on the number of users in each location instead with all locations. Again, clarify the discount schedule before committing.

Ease of Purchase — Deploying wireless devices is a bit different from deploying traditional telecom services. Traditional telecom services require hard-wiring equipment and a long process of provisioning. Wireless, on the other hand, can be deployed within a week. People don't mind waiting a few weeks to get their land-based phones installed. Yet, we are used to walking into a wireless store and coming out with a working phone in hand. When businesses purchase wireless devices, users expect to receive their devices immediately. If their phones were broken or lost, they expect them to be replaced immediately. Wireless carriers have different methods of distributing devices to businesses than to consumers. Some carriers have complicated requirements and procedures in place, so it may take weeks for the devices to arrive. For example, when the organization places an order, the carrier may need to verify the order was placed by an authorized person. Several forms and signatures may be required. And if the order was not placed correctly, either by the organization or carrier, the whole process may have to be repeated. Thus, as a customer, you need to understand the ordering process the carrier requires in order to avoid delays.

Invoice Format — Wireless invoices can come in several formats: paper, CD and online. Traditional paper invoices are most common, although they are being phased out due to cost and concern for the environment. CD-billing can replace the traditional paper invoice because it is more convenient and useful. Users can be grouped and their charges organized and billed back to each department. A summary can be printed and forwarded to accounts payable. Reports can be created for examining extraordinary usage or analysis of usage patterns. On the downside, a CD invoice may only be available anywhere from one week to three months after the billing period. When considering a CD-billing option, find out how long the CD is available after the billing period. Excessive charges or wrong plans may take longer to uncover and correct if the CD invoice shows up long after the billing cycle ends. Online billing details may be helpful to track usage immediately. However, larger bills may take too long to download. A more useful way to utilize online billing details is to make it available to the individual users to track current usage. Keep in mind that carriers may charge extra for any of these billing methods. Some carriers are already charging their customers for paper invoices.

Wireless Policy

Having assessed your wireless needs, picked a cellular technology and chosen a carrier, you should institute a

wireless policy to ensure that everyone understands what is expected when it comes to using their wireless devices. Items that should be included in the policy are:

Number of minutes each user is allocated

Handset selection criteria

Password-restriction on wireless devices

Level of access individuals have to the account (i.e., individuals can view usage details but not change plans)

International roaming guidelines

International calling guidelines

411 calls guidelines

Restrictions of data access on cell phones

Contact person for issues and questions

24/7 contact line for lost and stolen devices (provided by the carrier)

Employee-liable discount program

Accessories availability

Spare phones availability

Ongoing Wireless Management

Managing wireless does not end when a wireless program is put into place. Wireless rates (both voice and data) have dropped consistently in the past few years, but because carriers change plans frequently, it pays to periodically review your wireless accounts to make sure the plans are up-to-date. Also, the number of minutes put in place today may be insufficient a few months down the line. Other things to consider for your wireless management include: periodic invoice reviews to ensure correct billing and that proper discounts are applied; periodic technology updates from carriers; continual monitoring of the wireless industry for new trends and products; creation and maintenance of a database to track user information; monitoring handset upgrade eligibility; and user education sessions to assist with usage, roaming, damaged and lost/stolen devices.

Place That Call!

Completely reevaluating your wireless needs allows you to implement a wireless strategy and budget properly for the right amount of wireless service. Understanding the types of cellular technologies and devices available enables you to employ the right cellular technology and select the right carrier. A wireless policy is important to make sure users understand what is expected from them. Including wireless in the disaster recovery plan is recommended. When everything is in place, administer the wireless program to ensure technologies and services will meet tomorrow's needs.

About the Authors

Roger Bonine is IT Manager at Miller & Martin PLLC, a 180-attorney firm with offices in Atlanta, Nashville and Chattanooga. He has over 20 years of experience in the IT field as a software developer, systems engineer and manager. He holds several industry certifications, including Microsoft MCSE and Citrix CCA and has acted as lead designer on several large software development projects. Roger can be reached at rbonine@millermartin.com.

Apurva Davé is Senior Product Marketing Manager at Riverbed Technology, where he is responsible for bringing Riverbed's network infrastructure products to market. Prior to joining Riverbed, he held marketing positions at Fast Forward Networks and Inktomi, where he was responsible for network infrastructure market development. Apurva has an MBA from University of California, Berkeley and a Bachelor's degree in Computer Science from Brown University. He can be reached at apurva@riverbed.com.

Ray Deck is CEO of Element55, makers of the automatic time capture system, Legal55. Legal55 automatically populates attorneys' time sheets with time spent on phone calls, e-mail, documents, meetings and the BlackBerry. It captures with great accuracy and without having to start or stop a clock. Prior to founding Element55, Ray managed strategic and technical consulting organizations that focused on helping companies get more value from their data. He can be reached at ray@element55.com.

Athelene Gieseman is the CIO for Stinson Morrison Hecker LLP. She has spent over 19 years in law firm technology management. She oversaw the implementation of the firm's first IP telephony system in 2002 and a significant update of the system in 2005. Athelene is a member of the Cisco IP Communications Technical Advisory Board, Vice President of the Telecommunications Peer Group for ILTA and has been a speaker at the ILTA and ARMA conferences. Athelene can be reached agieseman@stinsonmoheck.com.

Faith M. Heikkila is a Pivot Group Security Consultant and currently a Ph.D. Candidate in Information Systems at Nova Southeastern University specializing in information assurance. She has over 18 years of paralegal and IT Project Management experience with two law firms in Michigan. She is a member of Association for Computing Machinery (ACM), Association of Information Technology Professionals (AITP), Computer Security Institute (CSI), Institute of Electrical and Electronics Engineers, Inc. and (IEEE), Information Systems Security Association (ISSA). Faith can be reached at fheikkila@pivotgroup.net.

Berylle Reynolds is a consultant with MBR Wireless Consulting located in Freehold, New Jersey. She has 10 years of experience in telecommunications, four of which in wireless data communications. She has a BS in Electrical Engineering and an MBA from The Anderson School at UCLA. MBR Wireless Consulting provides wireless management services for Philadelphia, New Jersey and New York areas. Berylle can be reached at 215.964.4500 or reynolds@mbrwireless.com.

Jack M. Sheekey is a Vice President of VideoTeleCon (VTC), recently merged with Courtroom Connect. The combined company is the leader in videoconferencing, video streaming, network connectivity and related services to the legal community. Jack is a frequent contributor to legal and technology publications and speaks regularly at industry seminars and conferences. His 20-year career includes a variety of marketing and consulting positions. Jack can be reached at jack@videotelecon.com.

Kristen Zarkadoolas is the Managing Director of Pivot Group, bringing over 10 years of leadership expertise, including management and operations, as well as sales and marketing. In this role, Kristen oversees global expansion, client relations, corporate communications and comprehensive market growth and profitability. Prior to Pivot Group, she developed a successful management career in the service industry. She can be contacted at kristenz@pivotgroup.net.

Disclaimer

This report is designed for use as a general guide and is not intended to serve as a recommendation or to replace the advice of experienced professionals. If expert assistance is desired, the services of a competent professional should be sought. Neither ILTA nor any author or contributor shall have liability for any person's reliance on the content of or any errors or omissions in this publication.

Copyright Notice

Copyright © ILTA 2005. All rights reserved. Printed in the United States of America. No part of this report may be reproduced in any manner or medium whatsoever without the prior written permission of ILTA. Published by ILTA, c/o Editor, 2110 Slaughter Lane, #115, PMB 149, Austin, TX 78748.



International Legal
Technology Association

2110 Slaughter Lane, #115
PMB 149
Austin, Texas 78748

PRST FIRST CLASS
MAIL
U.S. POSTAGE PAID
PERMIT NO. 1501
AUSTIN, TEXAS

• Address Service Requested

www.iltanet.org