Securing Telecommunications: Mission Impossible?

by Faith M. Heikkila, Kristen Zarcadoolas, and Ed Sale, 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-l 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.

*This article was first published in ILTA's November, 2005, white paper titled, "*Creating Omnipresence Through Telecommunications Technologies*," and is reprinted here with permission. For more information about ILTA, visit their website at www.iltanet.org.*