

[WP-014]

Whitepaper: Modem Use within the Healthcare Organization

How to Mitigate Risks of Legacy Systems Utilizing Modems (Known or Unknown)

Version 041101

November 2004

Author: Bob Radvanovsky, rsradvan@unixworks.com

(A special thanks goes to those listed for being my “sounding board” on this project.)

Copyright © 2004 Bob Radvanovsky. All rights reserved.



Limited Liability Statement

In no event shall the author(s) be liable for any found errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained within this document may be subject to change without any notice. No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this whitepaper.

Documentation pertaining to any security-related technical or proprietary information, its data and all information provided and contained within this document is considered proprietary in nature and subject to copyright protection and is intended solely for use by its owner. Additionally, this documentation is solely for discussing a possible, and/or proposed IT security issue, and is not dependent upon any specified infrastructure, architectural condition or its issue(s). Source information is through observation from previous employers, and discussions with colleagues within the IT security field, as well as observation at several local healthcare organizations.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners. NOTE: Any names not outlined or mentioned above are fictional in nature; as such, any relation to any name or trademark (if any) is purely coincidental.

What do modems have to do with ‘HIPAA’?

One of the risks that might be faced by any healthcare provider, organization or larger corporation is the question surrounding poorly configured modem connections that allow access to the internal network environments. By means of external access, just about anyone can find these modems using software easily found throughout the Internet. Some of the tools used not only discover the modems, but also attempt to break into the network by using some standard, generic, or default usernames and passwords. Once access to the network is established, these individuals can almost certainly (and quite easily) access other systems.

In many organizations, modems used are usually undocumented, unauthorized, or (in many cases) both. Policies about modem usage many times do not exist, thus to the end-user community, and the users that are supported by or through these modem, poses immeasurable, undiscovered/unknown dangers that the users may be unaware of, and how modems may be utilized against them within their environments. In other aspects, modems utilized on servers are considered “legacy systems”; that is, system environments that are entrenched/engrained within the very fabric of the corporate environments provide a supporting pillar to the organization’s profit and financial resource cash flow.



These systems are (many times) often out-of-date, and may use operating systems and architectures that are no longer supported (or were once supported) but now may be at the whim of companies that once supported them that are out-of-business, or have moved onto other platforms or architectures. In other words, these crucial, yet very critical, systems are no longer supported by anyone any more. One of the simplest (and effective) ways to controlling modem use is to simply turn them OFF. Modems are used only when needed, say for a vendor-supported upgrade, or an environmental fix. Modems should NEVER be open 24/7 UNLESS strong controls have been implemented. Some strong controls might be a modem pool with auditing capabilities, though rare, does exist. If, however, an end-user community relies upon the modem as a support mechanism “catch all”, for most enterprise solutions for many organizations, this is completely and utterly unacceptable.

The alternative to the modem...

Alternative measures to consider might include call back systems (systems in which users connect to a predetermined modem line connection, authenticate, then are contacted by the very same system after the initial authentication has been confirmed). This ensures that users and vendors from a predetermined list are authorized to access that system; but more importantly, allow for enhanced auditing capabilities.

If the modem was never noticed as being there before, the simplest method of remediation is (again) simply turning the modem OFF. When the end-user community and/or vendor supporting the architecture notice that they CANNOT access the server in question, the auditing issue becomes clarified; thus, if the vendor is listed within an established vendor list, then simply re-establishing that vendor's privileges to the server should not pose any issue. The vendor at this point simply accesses the server through a VPN client or tunneling mechanism. If the vendor is NOT on the established vendor list, the vendor must prove that they are authorized to access the server in question; otherwise, like a locked gate or door, it continues to remain closed and locked. Regardless, the modem should stay OFF.

What is a ‘VPN’?

The term “VPN” is not actually a term, but an acronym meaning “Virtual Private Network”. In the “Old Days” of computing, organizations would consider VPN tunnels as “extranets”, in which the company's network is simply extended to preferred vendors and customers via a highly-available, highly-secured and very expensive mechanism that tunnels an encryption “pipe” through an unsecured network – namely the Internet. To an end-user, having access to a corporate VPN means having a physical device, such as a key ring or token, along with a password, and a special software client that has been configured for the corporate environment's network. The end-user may access the VPN via a “portal” or “remote access point” in which there is a doorway into the company's network via a router or firewall (or some combination thereof). Once in, the end-user enjoys the same privileges of accessing the network as if they were at a workstation or desktop at one of the organization's operating centers, or at their own work desk.



Establishing a VPN tunnel employs the use of strong authentication (through encryption methods and a one-time password token, part of the “something that you have / something that you know” requirement in the authentication process).

The phrase “something that you have” represents a physical object, such as a key ring, token, key card, or some other physical item that is unique to the user attempting access. The phrase “something that you know” represents a password, key phrase, or combination of either. There is a third factor being considered: “something that you are”. This is representative of biometric mechanisms, such as eye, hand, or voice pattern recognition systems. Though there are ways to get around any given system (old computer science philosophy that there is no computer system that are entire “secure” [per se] may still continue to hold true, given sufficient time and beer), many organizations are considering biometric pattern recognition systems as an alternative – or even an additional requirement – as part of the authentication process.

Organizations should be aware of the risks that modem use creates and take whatever reasonable measures are required to mitigate these risks. These steps may include:

Identification of any modems in use (through use of any security tools).

One method of ensuring that modems are identified is by using a method called “wardialing”; that is, sequentially access each number within a given telephone numbering range or block of numbers, and performing a systematic and sequential search for any carrier found and established. Once found, the number is recorded, and if identifiable, recorded with the type of environment, and what weaknesses may exist (if any).

Ensure that only those that need access to modems have it.

Ultimately, if the corporation or organization is currently utilizing VPN technology, consider using that in lieu of modems. If the corporation or organization hasn't considered utilizing VPN technology, many companies today offer competitive pricing for enterprise-wide solutions that are more reliable, more secure, and similarly priced.

Monitor dial-in attempts (especially failed attempts) and investigate their origins.

This would require the use of a telephone sniffing or tracing mechanism. Unbelievably, simply turning OFF the modem is far more effective, esp. when management and/or security personnel are unaware of where the modem is located, or who may be using it.

Create a policy to ensure only authorized modems are included in your network.

The policy should be simple: for any access into the organization's internal environments, use of strong authentication (through encryption) is necessary (i.e.; use of VPN private networking technologies). No modems may be attached to any internal device – period – due to the inherent risk of exposure to external communications lines that may be unprotected and (more importantly) unmonitored.



Ensure authorized modems are configured and have sufficient controls in place.

Some may argue that modems are necessary to the organization. If circumstances present themselves in such a manner, such as this, provide the end-users who are arguing their point in providing a financial reason as to why the organization must be exposed to external connections that are NOT monitored (and for that matter, usually CANNOT be monitored), and CANNOT be easily secured (aside from simply turning them off). If the end-users or vendors questioning the need for modem dialing capabilities are necessitated, present them with a VPN solution instead.

For many healthcare organizations plagued with physicians dictating how the IT department(s) should run or operate, through observation, physicians have been noted to be stubborn towards any technological change, esp. if it requires significant workflow modifications. That is, if the process requires additional time (and with any newer technology, there is always a ramp up timeframe that allows end-users to get accustomed to the newer technologies), most physicians will often balk at its implementation, requesting that the “old system” be put back into place. Given the political structure within the healthcare organization, many physicians will (more often than not) win at this game; however, if given sufficient tools (if you will, “weapons”) to combat this problem, present the physicians that are objecting to the newer technology to “sign off” through a waiver. If they still insist on utilizing the “old system”, have them “sign off” (again) on a different waiver, disclaiming any liability or privacy issues that will arise from exposure to external communications sources, also stating that the physician assumes all legal liability for monitoring and maintaining these environments. Once put into legal terms, the physician will suddenly have a change in heart, and go with what is recommended from earlier.

It was addressed by a fellow colleague who knows several physicians that the physician in question would simply stall and ‘stonewall’ the signoff process of the waiver until infinity. However, given the ramifications of HIPAA and what it could potentially do in destroying credibility and reputability of both the healthcare organization and the physician in question. Having an audit trail of memorandums, electronic mailings, etc., the organization (ultimately) wins over the physician as any and all electronic messages are stored and saved – as long as the organization shows due diligence – the process will vindicate the organization of any wrong-doings, demonstrating that it is making an effort to be “HIPAA Compliant”.

Though this shouldn’t be a matter of ‘us’ versus ‘them’, medical doctors oftentimes think of their efforts in a ‘godlike’ manner because they save lives, and that everything is second nature to it. Many physicians must realize however, that with any healthcare organization, its sole purpose is not in the business of saving lives, but of making money (which, unfortunately, is also the main objective of medical physicians, too).



The physicians' arguments are a time saving measure – in many cases, being expressed by the nursing staff that supports the physicians. Physicians argue that they want:

- an ability to get information to remote users faster;
- more secure methods in identifying remote access users;
- an ability to integrate existing network environment without customization;
- flexible capabilities that offer users a secure, remote access capability from virtually any terminal or PC within or throughout the organization;
- a system that is easy to manage without a lot of additional administrative overhead;
- and (most importantly), the ability to expand and meet future remote access requirements, including the use of digital certificates.

With greater exposure to the Internet through broadband capabilities, increases throughput from various service providers both within and throughout the United States, many healthcare providers will see cheaper solutions that will provide the necessary requirements of ensuring privacy, security and patient record safety (and its integrity). Obviously, utilizing VPN technologies will only improve as they continue to speed up and enhance on-demand patient record keeping capabilities.

Over the next several years, many anticipate seeing the exchange of documents with outside partners and vendors that will require the use of digital certificates. Healthcare providers may decide to choose this operating method, partially because these organizations won't have to replace the technology after their need for identifying any different or newer authentication technology has already been performed.

Thus, the VPN capability will make life (much) easier for many physicians and their staff. Physicians that have access capabilities for accessing patient records from just about anywhere are becoming confident that adding a protective layer involving strong authentication and encryption will protect the privacy of their patients, while at the same time, ensuring that requirements of HIPAA have been met.

Are there any remote access technologies available?

There are plenty of solutions to choose from; however, not all solutions are secure.

One prime example is Symantec's PC Anywhere. This solution allows remote access capabilities to any given Windows platform. In many cases, this product is utilized by system administrators and/or support staff to maintain the server in question. However, in most cases, use of this product signifies an "all or nothing" granting of privileges, often exposing the company's networks to huge holes, and inviting uninvited external visitors to wreck havoc on internal networking Windows servers.

Since not all environments are Windows-based, there will be other architectures, such as Novell's Netware, various UNIX and LINUX platforms (too many to list, but you know who they are), DEC's OpenVMS, WANG, and of course, the "Big Iron" box itself – the IBM mainframe. For a mixed architecture environment, Symantec's PC Anywhere solution won't work, so there are some alternative solutions.



One is Citrix Systems Metaframe/XP, the other is Cisco's VPN client. In both circumstance, the software used is by the end-user utilizing a client software that is pushed down after authentication. There are numerous methods of ensuring that end-users can or cannot perform specific functions; however, observation of industry standards, reliability, data/network integrity and (overall) security have found these two access methods most useful. One is via a secured web (HTTP) interface (Citrix); the other is simply through a closed-architecture secured portal client (Cisco). Depending upon the size of the audience, one may be more suitable than the other. In some cases, I have found large corporations to utilize both methods of remote access.

In either case, both methods have been found to be fairly reliable and secure.

