



Vol.6 Number 8
July 2006

Phone Security: Protecting Reliability and Privacy in Today's World

Most organizations today list information integrity as one of their greatest concerns, and they go to great lengths to protect and secure their corporate data assets. But what many fail to realize is that voice communications are just as important, and therefore can be just as great a liability, as other electronic information within the company. The reliability and privacy of voice communications must be maintained. But what voice technology platforms are best and what can you do to ensure the integrity of your own important phone calls?

VoIP vs. Traditional Phone: Which is more secure?

There is a common perception that VoIP (Voice Over Internet Protocol), based on the open standards of the Internet, has increased security vulnerability over traditional phone systems, particularly when it comes to the issue of intercepting a conversation. In actuality, this is not the case.

VoIP is based on technology that converts your voice into data packets that are in turn sent over your network along with conventional corporate data. In order for a conversation to be intercepted, an intruder first must gain access to the local area network. The intruder must then hope the VoIP vendor uses a standard compression algorithm that he has the ability to decode. Keep in mind, one voice packet will only have a fragment of an actual conversation. Unless someone can intercept and decode all of the packets, the possibility of corporate espionage is remote.

Now compare this to a traditional phone network. TDM (Time-Division Multiplexing) is the older technology commonly employed by many companies. TDM is a closed circuit-to-circuit system, meaning that if someone taps into the system they will have access to every outbound conversation in the entire building. And they will need a comparatively simple level of technology in order to do it. When you look at the complexity involved between breaching a TDM system or breaching a secure VoIP system, VoIP quickly becomes a very attractive option.

But there are some very real security risks that must be considered when deploying VoIP. The good news is that these are probably the same risks that your company has been dealing with for years. Rather than the interception of a voice communication, the more prevalent security risk with VoIP is that of a malicious, generalized attack. If an attacker deploys a virus or worm to your corporate data network, then it will affect your VoIP communications as well.



A second type of common threat is a direct attack from someone within your organization, such as a disgruntled employee. This type of person might have access to the proprietary technology that your VoIP solution is deployed on, and they can tailor their attack to match the vulnerabilities of the system

What can you do to enhance security?

Your IT department probably already has multiple security measures in place to protect phone communications, especially in the case of offsite remote users. The best advice we can give is that when your IT staff gives you extra security procedures to follow-follow them diligently.

Your company might deploy a Virtual Private Network to tunnel their remote users through the public Internet system. You might also be given remote user verification devices such as biometric systems or remote security keys with randomly generated passwords. The reality is that these types of protocols might limit your access to certain features or functionality on the network, and there might be extra steps involved before you are actually able to make a call. While this process may seem like an interruption in your daily workflow, there is a payoff in reliable and secure phone communications that is well worth the effort.

Additionally, you must always keep an eye on internal threats. The same HR policies that protect your company from fraud and other criminal issues can be used to protect your phone system from attack. You should keep your phone system and data center under lock and key. Background checks, access limitations and personnel screening are all effective methods to keep your private phone conversations private, and to maximize uptime for your phone system. And in the long run, these are steps that we should all be taking to ensure a safe and productive working environment.