

## Hold Onto Your Pigs, Security Isn't Fixed- Will It Ever Be?

PRINT

February 06, 2007

By Matt Brunk

I pulled some dusty newsletters to an IP-PBX dealer community and came across "Quotable Quotes" dating back to 1Q, 2003.



*"IP-PBX vendors are responsible for secure VOIP communications, IP-PBX vendors are responsible for security vulnerability in the operating system they choose as their platform, and IP-PBX vendors are responsible for providing a well designed IP stack."*

**Kenneth M. Percy & Randall E. Birdsall, Miercom**

Does this mean interconnects, VARs, or the PC guru wanting to sell cheap telephony solutions to increase his margins or customer's dependence will in fact own responsibility of surfacing security issues including the known vulnerabilities? Perhaps the big guns at Avaya, Cisco, Nortel, and Siemens will take complete ownership without the caveats of "if and but, excluding or limited to, etc."

But then you probably believe that pigs can fly.

Maybe I'm cynical but history teaches us that for a very brief time some of the vendors were in fact liable for customers toll fraud losses due to their RMATS, remote modems and other telephone maintenance "functions" left unsecured. History also teaches that not many recovered all their losses even when their carriers were forgiving. How forgiving, well just ask the flying pigs.

Now that L-enterprise is in hot pursuit of the IP-PBX and jack-in-the-box phone solutions, a little more attention has been thrown at security. Last year an industry expert cited that most networks aren't secure because the infrastructure is weak or designed wrong. It seems that with every issue (problem) related to the IP-PBX or VoIP, that a new gizmo or solution is introduced. Someone else pointed out that to trust that Microsoft will fix their own security issues and vulnerabilities would mean an end to firewalls, security software and many other wares that go into the TCO expense pile labeled as security. I think I just saw another flying pig.

Just like I asked the "infrastructure expert" I'd ask the same to any manufacturer- "how secure is secure?" This gives plenty of wiggle room. Skeptic or cynic may come to mind but until you've had your first thrill ride down security lane, you may remain doubtful even skeptical or cynical and believe in your product or solution.

Some of the best advice in 2003 was published in BCR's February issue on page 4.

*"Enterprises aren't going to replace paid for TDM-PBXs until they have to...as important as it is for vendors to have robust, feature-rich, secure IP-PBXs. Why not use this time and resources to create world-class IP-PBX software?"*

**Eric Krapf, BCR**

What really matters is Eric's point about "world-class." On that day and in the moment of each user's reading of that article "Security, Software And Voice" was a bench mark set. Now four years later- who can claim "world-class" success? I do agree that the industry has delivered on robust and feature rich. Two out of three isn't bad but security still isn't an option. Just how secure is "secure" in your definitions and how responsible are the manufacturers or installing/servicing companies? The demarcation isn't the only thing that is soft. The breadth and width of security may yet be pretty fuzzy and one thing remains certain about IP-PBXs and VoIP security, they remain vulnerable. How we move them into world-class is a challenge still unfulfilled and it seems that the "how" is what customers and prospects need to know more about.

## Comment on this Article

[Click here to comment... \(Show/Hide Form\)](#)

## Other Visitors Comments

There are no comments currently....

**Close Window**