

» [Subscribe to Tech Decisions](#)

[RSS Feeds](#) | [Advertise](#) | [Contact Us](#)

# Techdecisions FOR INSURANCE

Career Center Powered by [GreatInsuranceJobs.com](#)

 

[Home](#) [Magazine](#) [News](#) [Topics](#) [eNewsletters](#) [Supplements](#) [Personalities](#) [Web Seminars](#) [Calendar](#) [Directories](#) [Podcasts](#) [Subscribe](#)



**Faster claims resolution = happier clients = lower LAE. With ImageNow, you can have it all.**  
 Discover document management efficiency at [www.imagenow.com/insurance](http://www.imagenow.com/insurance)

Article

## Internet Telephone Service: A New Frontier For Insurance Carriers

BY **HARRY EMERSON**

Published 1/18/2010

[Subscribe to Tech Decisions](#)

[Email Share](#)

[Print This Article](#)

[Normal Text](#)

[Large Text](#)



Harry Emerson  
Emerson Development

At a time of economic downturn when insurers are struggling to grow revenue, the security issues generated by Internet phone service, aka Voice over Internet Protocol or VoIP, could very well create a new frontier for insurance carriers.

Most of you are familiar with the popular Internet phone service known as VoIP, a low-cost, discounted service that is rapidly being adopted just about everywhere. The use of VoIP telephones is growing because of their generous price structure and the relative ease of entry for new users. But there is a dark side to nearly-free telephony which has escaped our general attention as we joyfully embrace its ever-cheaper cost of doing business. Unfortunately for the user, society will be noticing this dark side more and more as organizations and institutions across the globe continue to adopt VoIP for their primary means of telephone communication. Lured by the siren call of low cost or no-cost service, and the absence of any FCC regulations whatsoever, the public and private sectors have closed their collective eyes to the glaring absence of safeguards built into this cheaper / cheapest business model, and like lemmings are enthusiastically racing towards the cliff of cyber-insecurity.

What we are not looking nor seeing is that in the process of changing over to VoIP, users are unwittingly shifting from the reliable and secure traditional telephone network to an Internet environment of extreme risk. As it becomes more prevalent, we anticipate that VoIP will be increasingly vulnerable to hostile acts. This is because due to the architecture of the Internet, every person and every system has direct access to one another, implicitly giving all of us a trusted relationship with every hacker and terrorist in the world. By joining the VoIP party, we not only give those with malicious intent the direct access to our existing systems, computers, and networks—which we have already conceded—but we extend that access into the private realm of telephone communications.

The honeymoon is over. It is now being recognized that friendly, affordable, easy-to-use VoIP shares all the risks of the Internet, exposing all the features of voice communications to hacking and exploitation with the potential for disastrous results.

This is bad news for VoIP users, but indications are that it will be good news for insurance carriers who will be called upon to protect against the risk of financial loss by VoIP users, VoIP manufacturers, VoIP distributors, installers, designers, and sellers. Consequently, according to Glenn Tippy, president and managing partner of Gerrity, Baker, Williams Inc. ([www.gbwinnsurance.com](http://www.gbwinnsurance.com)), and board member of the Professional Insurance Agents of New Jersey Inc., we can foresee that “insurance carriers will increasingly price for Internet / VoIP telephone exposure; cyber insurance products will be created for users of VoIP, as well as for VoIP providers and vendors; and The effects upon our economy will be profound.”

What we are talking about is a major shift in the perception of safety vs. risk as the hazards built into the current VoIP system are acknowledged. We are also talking about a major new market opening for insurers.

We are not alone in our assumption of perceived risk. With businesses and government spending vast amounts of money to protect themselves against what feels like a growing army of terrorists invading the technology we all depend upon, the Obama administration is rightfully zeroing in on cyber security, cyber crime, and cyber warfare



### Recent Issues

- [December](#)
- [November 2009](#)
- [October 2009](#)
- [September 2009](#)
- [August 2009](#)
- [June, 2009](#)
- [MAY 2009](#)
- [APRIL 2009](#)

### ARCHIVED ISSUES

### Most Read Articles

- [Accounting Super Session Tackles Tough Topic of Standards Convergence](#)
- [Internet Telephone Service: A New Frontier for Insurance Carriers](#)
- [Product Configuration at the Heart of your P&C Policy Admin System](#)
- [The Next Step in Tech: One Click Reconciles Producer Data with Records in Every State Under Your Nose](#)

### Related Articles

- [Reduce Operating Costs and Increase Underwriting Efficiencies by Rationalizing Your Product Portfolio](#)
- [Thank You](#)

as a major part of its homeland security priorities. Meanwhile, the situation is getting worse, not better, which is why it has now been elevated to the level of a national security concern. Should we be worried about Internet phone service as it is now configured? Unfortunately, the answer is “Yes.”

Being server-based, Internet telephony is susceptible to espionage, hacking, eavesdropping, intrusion, interruption, identity theft, denial-of-service attacks, and other forms of malicious and criminal interference via any and all the techniques that hackers employ. The role of hackers is to devise schemes to break into Internet servers. Therefore, no one should be surprised that with the accelerating trend towards widespread use of VoIP technology, they will turn their attention to VoIP servers. All Internet servers are susceptible to hacking. The fact that VoIP relies upon servers accessible on the Internet endangers personal, corporate, and national security, which will have a direct and increasing impact upon the insurance industry and those it serves. “VoIP is making it easier to wage cyberwar...” an analyst reported as far back as 2004, “just as flaws that make some VoIP products vulnerable were revealed.” - (Network World 1/19/2004). The growth in malware and cyber attacks is exponential. According to F-Secure Corporation, malicious software attacks tripled in 2008<sup>[1]</sup>. Midway through 2009 McAfee's Avert Labs reported that attacks have tripled since 2008.

We have begun to see many examples of cyber crime including the exploitation of VoIP throughout society and the world. Two extreme cases are now recognized as early warning signals: In 2007 Russia utilized cyber-warfare against Estonia and in 2008 against Georgia, and completely shut down the infrastructure of those countries. More to the point for the insurance industry, according to a recent report by the security firm McAfee and Purdue University, theft of intellectual property, fraud, and damage of corporate networks cost corporations over a \$1 trillion globally in 2008. To give this discussion more focus, think about the implications for the legal profession, the banking industry, hospitals, pharmaceutical companies and medical practices, the non-for-profit sector, manufacturers, governments, the military, and private individuals as they migrate to VoIP in greater numbers; and consider the impact on the insurance industry as client losses due to VoIP begin to pile on top of that \$1 trillion.

The rise of the Internet has produced something akin to a gold rush mentality for those mining its resources and developing its vast potential. The lure of easy money has caused nontraditional carriers to provide customers with VoIP services, which, as stated earlier, in many cases are nearly free. In addition, VoIP companies such as Skype, Vonage and the various cable carriers (Comcast, Time Warner, and Cablevision), have ventured into Internet telephony not only to provide cheaper communications, but also to avoid regulatory scrutiny, the absence of which also lowers cost. However, in the midst of the frenzy we have turned a blind eye to fundamental requirements for privacy, secrecy, and security and we now must prepare to face the consequences.

Meanwhile a growing backend industry is developing to create piecemeal fix-it technologies which are costly to plan, to acquire, and to administer, and which will be unavoidably inadequate due to the very nature of VoIP. It might be possible to harden some pieces of infrastructure that an organization has control over (keeping in mind that most small entities will not have control over anything), but you can't protect against VoIP calls to or from locations outside those boundaries, nor can you protect against public systems on the Internet such as DNS (domain name servers). And you certainly can never protect against risks such as eavesdropping when the other party uses VoIP (whether or not you do) because you have no way of knowing if their systems or service providers have been compromised. Furthermore, hardening doesn't prevent the possibility of an employee contracting a virus or Trojan horse that can share all your phone calls with an invisible third-party.

However, at Emerson Development, we advocate planning for features and services incorporating front-end provider-based security by enhancing the existing public telephone network to support broadband Internet connections. That plan can be seen and studied [here](#).

Meanwhile, the flourishing VoIP online telephone service will soon be recognized to be broken. Protections will be needed for the inevitable problems arising for the growing numbers of VoIP hardware and software developers, carriers and end users. The insurance industry will have its work cut out for it in a profitable new arena focusing on the telephone sector of Internet communications and the issues of cyber-security.

[1] [http://www.f-secure.com/en\\_US/security/security-lab/latest-threats/security-threat-summaries/2008-4.html](http://www.f-secure.com/en_US/security/security-lab/latest-threats/security-threat-summaries/2008-4.html)

**About the author:**

*Emerson Development founder and managing partner, Harry Emerson, is an expert in computers, voice and data communications, and the Internet. His career history includes 25 years in various management and strategic capacities at AT&T and the design and management of large-scale, multi-million dollar enterprise applications and data systems. His most recent project is the development of a plan to modify Online telecommunications on the provider side, so that the Internet's broadband capabilities can be used without jeopardy.*

Contact: Jacqueline Herships Communications  
973-763-7555 [jacqueline@jacquelineherships.com](mailto:jacqueline@jacquelineherships.com)

June 2006

June 2006 - Tech Decisions Magazine

Out on a Limb—With Company

IT Cowboys

Ask Dr. G.

Is It Real, or Is It Virtual?

Big Benefits for Small Term

Ohio Casualty Speeds Agency Download

Capabilities

St. Paul Travelers Adds Enhanced Dashboards

on Electronic Portal

UnumProvident Offers Electronic Claims

Monitoring Service

It's Life's Turn

Company: iPartners

Glatfelter Insurance Group's Wayne Umland

The Alignment Myth?

## COMMENT ON THIS ARTICLE

Name:

Email (will not be published):

Subject:

Comment:

Type the two words:

Submit Comment



**Faster claims resolution = happier clients = lower LAE. With ImageNow, you can have it all.**  
*Discover document management efficiency at [www.imagenow.com/insurance](http://www.imagenow.com/insurance)*



Summit Business Media  
 5081 Olympic Boulevard  
 Erlanger, Kentucky  
 41018

### Site

- Home
- Magazine
- News
- Topics
- eNewsletters
- Supplements
- Personalities
- Web Seminars
- Calendar
- Directories
- Podcasts

### Magazine

- Subscription
- Current Issue
- Directories
- Editorial Guidelines
- Editorial Calendar

### Resources

- Reprints
- Advertising
- About Us
- Contact Us
- Career Center
- Media Kits
- Press Releases
- Site Map
- Privacy Policy

### RSS

View and create **RSS feeds** from Tech Decisions Magazine.