

VoIP: Are fools rushing in?

What does it mean to insurance if they are?

By Harry Emerson

More professional insurance agents are discovering the nearly free telephone services that are available via the Internet. Attracted by low cost of entry; ease of retrofitting; scalability; and lack of rules and regulations governing online telephony, businesses are rushing to use the Internet as their platform of choice for telephone service. It almost seems too good to be true, which could mean that perhaps it is too good to be true. And so, if for no other reason than to undertake proper due diligence, agents should ask: Is there something wrong with this picture? How can a communications technology, which always has produced regular, hefty line items on the budget, suddenly become so inexpensive? Is this telephone panacea for real? Or are hidden problems lurking beneath the surface, waiting to emerge?

Perhaps a bit of both.

However, this is the direction in which society is moving and at the moment few are looking at the big picture. Online telephony is real, it's cheap, and judging by the current rush to participate, most users love it and are satisfied with it.

This new wonder-system, known as Voice over Internet Protocol, or VoIP, is a form of Internet telephony defined by Wikipedia as a "general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks" ... and refers "to communications services—voice, facsimile, and/or voice-messaging applications—that are transported via the Internet, rather than the public switched telephone network." (<http://en.wikipedia.org/wiki/Voip>)

In short, VoIP provides a neat package of services that are attractively priced and which are becoming less expensive as time passes. Understandably, momentum is building as VoIP is embraced within every sector of society (e.g., the legal profession, the banking industry, hospitals, pharmaceutical companies and medical practices, the not-for-profit sector, manufacturers, the military, governments and private individuals) in greater numbers. However, individual consumers may not be aware that the phone service advertised by some providers is carried on the Internet. Recent ads pitch a bundled package of television, Internet access and phone service, without mentioning that the phone calls use the Internet rather than the public switched telephone network.

On the provider side, the ability to offer low- to no-cost telephony is more or less irresistible. There is money to be made with VoIP. Companies such as Skype, Vonage, the various Cable carriers (Comcast, Time Warner and Cablevision), are jumping onto the Internet telephony bandwagon. Contributing to the enthusiasm generated by the current low cost environment is the Federal Communications Commission's decision to interpret VoIP as "data communications," because data communications are not subject to telecommunications regulations. Since studying and adhering to regulations is expensive, the absence of such regulations indirectly enhances the bottom line, at least in the short term.

This exciting, freewheeling environment is the source of our problem.

Provisions for security are essential if communications are to flourish. But the Internet is not secure. It is important to understand that the architecture of the Internet initially was created by trusting academics and scholars, for the purpose of connecting with each other to share information. This open architecture still is in place, which means that every person and every system that uses the Internet still have direct access to one another. Therefore, under the current arrangement, we all implicitly have a trusted relationship with every hacker and terrorist in the world. This means that VoIP telephone systems are vulnerable to the same sorts of attacks as are any Internet-connected devices. Hackers who are aware of these vulnerabilities can initiate denial-of-service attacks; extract customer data and intellectual property; intercept and record conversations; and engage in spying and theft activities such as breaking into voice mailboxes.

On one hand, as costs continue to come down; competition grows more fierce; and return on investment becomes more slim, there will be even less incentive to remediate these inherent vulnerabilities, which have been left for the user to handle. On the other hand, we expect the security issues generated by Internet phone service to create a new frontier for insurance carriers.

The issues of risk management, which we predict will emerge, can be understood by contemplating a basic list of questions compiled by Insurance and Risk Management specialist, R. Scott Wolff of Premier Risk Management LLC, for Emerson Development's upcoming *VoIP Security Review—Insurance*.

E-mail at PIA

Each PIA department has its own e-mail address:

General

pia@pia.org

Conferences

conferences@pia.org

Creative Services

creativeservices@pia.org

Education

education@pia.org

Government and Industry Affairs

govaffairs@pia.org

Industry Resource Center

resourcecenter@pia.org

Member Services

memberservices@pia.org

Publications

publications@pia.org

Spanish marketing materials

creativeservices@pia.org

Young Insurance Professionals

yip@pia.org

Please keep these addresses handy to reach PIA electronically.



Think **PIA** first

This report discusses Internet-based telephony as an anticipated producer of major losses in cyberspace, a new frontier for those in the insurance industry.

These questions are:

- 1.) What are our risks? Conduct a thoughtful analysis to identify company risk.
- 2.) What are the threats?
- 3.) Where are we exposed?
- 4.) Ask: If this happened ... how would it affect our flow of business?
- 5.) What would the financial impact be on our business if this happened?
- 6.) Do we have contingency plans in place?
- 7.) How will our insurance policies respond? Are there gaps?
- 8.) What would be the cost to remediate the system/security?
- 9.) What can we implement to prevent an occurrence from happening?
- 10.) Can we implement a disaster recovery program in case an event occurs?

If, as we predict, Internet telephony creates exposures that become major loss producers, emerging armored technologies to protect Internet telephony, such as Emerson's IronPipe™, will have a role in mitigating these exposures. Meanwhile, members of the insurance industry will monitor carrier changes to relevant coverages and insurance counselors will recommend the full range of available extensions of coverage for cyber liability as it applies to telephone over the Internet. We advise all interested parties to be watchful and stay tuned. ■

Emerson is a 25-year expert in computers, voice and data communications and the Internet, and the founder and CEO of Emerson Development LLC. His most recent project is the development of a plan to modify online telecommunications, which bypasses hazardous VoIP architecture completely, thus making use of the Internet's broadband capabilities without jeopardy. An audio-visual presentation describing Emerson's IronPipe security system is available on the Web at www.emersondevelopmentllc.com/Assets/TelecomPresentation.html.