

# Internet Security Systems

2006 Survey: The State of Security  
In Carrier Service Delivery

## Executive Summary

Internet Protocol (IP)- and wireless-based communications are driving the next-generation business model for carriers worldwide. Triple Play (data, voice and video) and Quad Play (Triple Play plus wireless) service bundles make it possible, for the first time, for a single service provider to “own the pipe” delivering all communications services into the customer premises. Thus, there is a de facto arms race between telecommunications and broadband carriers to roll out these new service bundles as quickly and effectively as possible.

The initial goal of this arms race has been to create commercially viable services. And, the biggest initial challenge has been to develop services that can meet customer requirements for quality and reliability. Since customer expectations have been set by the quality and reliability of the traditional telephone network, this is a daunting task.

The reliability and quality of Voice over Internet Protocol (VoIP) telephone service must approximate that of traditional phone service if it is to enjoy mass adoption. Wireless faces a more forgiving audience due to customers’ willingness to tolerate lesser quality in exchange for mobility. However, as fixed-mobile convergence merges wireless and VoIP communications and enables people to move to a model of “one-phone, one number,” wireless too faces a world of increasing quality and reliability demands.

The same dynamic holds true with IP-based television (IPTV) services, where customer expectations have been set by traditional cable television. And while the “cable man” has been the butt of consumer jokes for decades, the network itself has delivered highly reliable services over the years. Thus, to roll out new Triple- and Quad-Play services, carriers have been challenged with leveraging the Internet to radically improve the capacity and flexibility of a network that was never designed to carry voice or video.

This laser-focus on reliability and quality, however, has been done largely at the expense of security. Security simply has not been built into IP or wireless communications protocols, and as these new services

gain increased adoption, they will become an increasingly attractive target for the cyber-crime organizations currently targeting the data networking world. The industry is already seeing the first instances of this with VoIP-based phishing attacks, wireless malware and other early attacks. It is almost certain that these and other attacks will become more widespread as these technologies proliferate.

With the rollout of Triple- and Quad-Play services, carriers are elevating security issues to the top of their technology agenda. However, with the threats also comes opportunity: while building an infrastructure to secure their own service offerings, carriers can also offer security as a new subscriber service. Colloquially called “in-the-cloud” security services, this works by customers routing their network traffic through the service provider’s security infrastructure, where it performs security services and delivers clean traffic to the customer. As enterprises seek to outsource much of their security functions, these new services represent a large potential market for carriers.

To gain more insight into the state of carrier security, IBM Internet Security Systems recently held a carrier summit to examine emerging security threats and opportunities. The summit was attended by more than 50 managers and executives from some of the world’s largest carriers. As part of the proceedings, IBM Internet Security Systems surveyed these carriers on their security strategies and found some revealing statistics, including:

- 55 percent said that security issues were impeding their rollout of Triple- and Quad-Play service bundles.
- 78 percent said that VoIP services will fail without strong security.
- 78 percent said in-the-cloud security services will become a major revenue generator within five years, yet 49 percent said they do not have the core competency to deliver these services today.

The following sections detail the survey questions and responses.

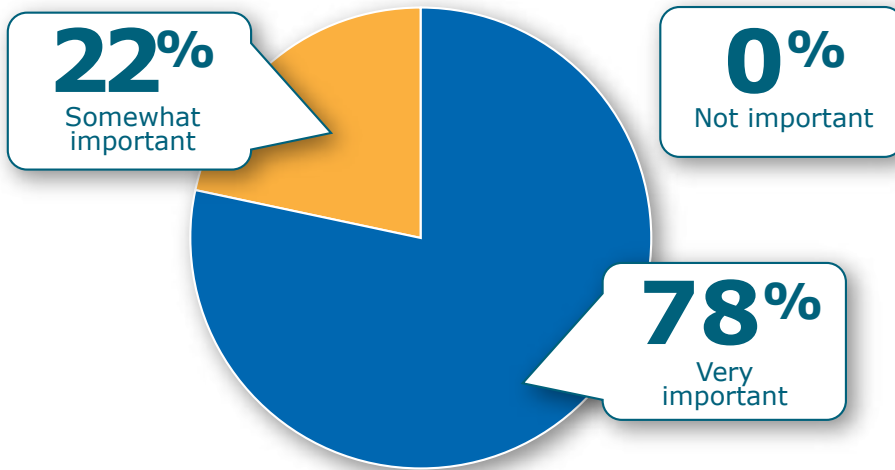
## Security and Service Rollout

Survey respondents indicated significant concern around security issues and new service rollout. The majority indicated that security could threaten the long-term viability of new IP-based services and almost half said that

hackers with limited technical knowledge can compromise these services today. Following are specific responses to survey questions.

### Question 1.

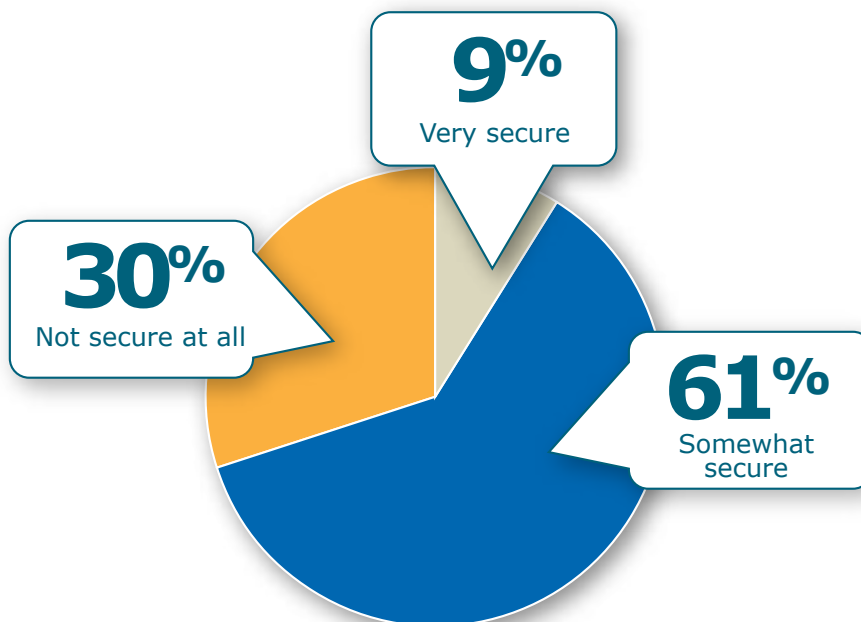
How important do you feel VoIP security is to the long-term viability of the VoIP services?



Perhaps most interesting in this question is that no respondents dismissed security as a concern for VoIP. When one considers the comparison point for VoIP – the relatively invulnerable and strongly policed traditional phone network – this response makes sense. If security becomes a problem for customers, then they will revert to traditional phone service where in their experience there are no real security concerns.

### Question 2.

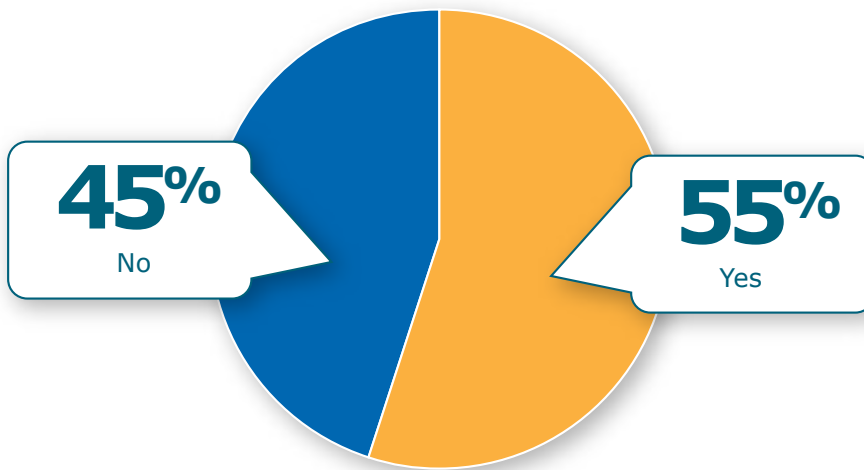
In your opinion, how secure are initial IPTV rollouts?



Respondents were clear on this question – nine out of 10 said that IPTV services are somewhat secure or not secure at all. 30 percent indicated that any garden-variety hacker could penetrate IPTV today.

**Question 3.**

Are security issues impeding you rollout of Triple- and Quad-play bundles?



Getting to the crux of the matter, more than half of respondents said that security issues were impeding their ability to roll out their next generation services. Ironically, widespread adoption of these services will make them a more attractive target for cyber crime organizations, so the potential threat will increase as services gain traction.

## In-The-Cloud Security Services

Responses to questions about in-the-cloud security services revealed a gap between strategy and ability to execute. 78 percent predicted that in-the-cloud security services would be a major source of revenue within five years, but only two-thirds of respondents said they had a strategy in place today for delivering in-the-cloud security

services, and only 51 percent said they had the core competency to do so. This would indicate that carriers are going to expend significant resources in the next few years on developing and rolling out these services, since many are not prepared to do so today.

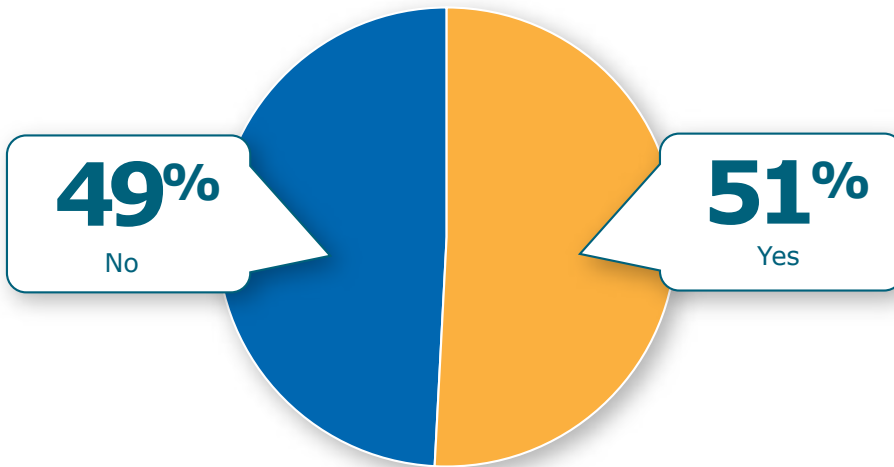
**Question 4.**

Do you have a strategy for offering "in the cloud" security services to your customers?



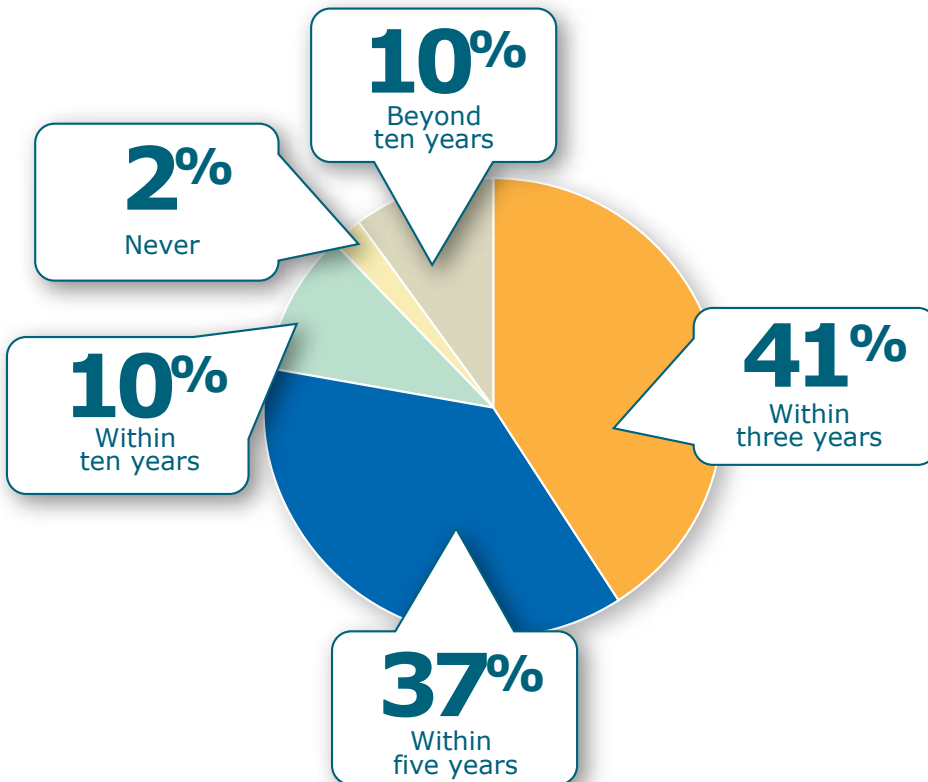
**Question 5.**

Do you have core competency to offer in in-the-cloud security services today?



**Question 6.**

When do you think in-the-cloud security services will become a major revenue generator for your company?



## Security Rises to Strategic Importance for Carriers

Carriers stand on the cusp of a new era of next-generation services. As technology matures and quality and reliability issues subside, security is emerging as the final roadblock standing in the way of service rollout and market acceptance. Likewise, because security has become such a pervasive concern for carrier customers, security also represents a major new business opportunity through in-the-cloud services.

The results of the IBM Internet Security Systems survey indicate two clear challenges:

- Carriers must improve security around inherently insecure protocols if IPTV, VoIP and fixed-mobile convergence offerings are to become a success in the marketplace.
- Carriers must build out their infrastructure and internal expertise if they are to meet their business goals for in-the-cloud security services.

How carriers respond to these challenges will determine the winners and losers in the arms race for delivering next-generation services.

## About IBM Internet Security Systems

IBM Internet Security Systems is the trusted security advisor to thousands of the world's leading businesses and governments, providing pre-emptive protection for networks, desktops and servers. An established leader in security since 1994, the IBM Proventia® integrated security platform is designed to automatically protect against both known and unknown threats, helping to keep networks up and running and shielding customers from online attacks before they impact business assets. IBM

Internet Security Systems products and services are based on the proactive security intelligence of its X-Force® research and development team – the unequivocal world authority in vulnerability and threat research. The Internet Security Systems product line is also complemented by comprehensive Managed Security Services and Professional Security Services. For more information, visit the Internet Security Systems Web site at [www.iss.net](http://www.iss.net) or call 800-776-2362.

###

*Internet Security Systems is a trademark and Proventia and X-Force are registered trademarks of International Business Machines Corporation in the United States, other countries, or both. All other companies and products mentioned are trademarks and property of their respective owners.*