



2007 Survey: The State of Security in Carrier Service Delivery

Executive Summary

For the second year in a row, IBM Internet Security Systems™ has conducted a survey of telecommunications carriers to understand their opinions, practices and plans regarding security.

The 2007 survey revealed that the wholesale migration to next-generation Internet Protocol (IP)-based architectures is imminent, with almost 85 percent of respondents indicating that they will roll out this kind of architecture in the next five years.

This has interesting security implications since IP is a well understood and highly exploited protocol. This means there is already a large population of cyber-criminals and other miscreants capable of compromising IP-based communications channels. Thus, the migration to next-generation IP architectures stands to provide an enticing new target for these attackers.

It is not surprising that 87 percent of survey participants indicated that next-generation networks (NGNs) will fail without strong security. However, fewer than half of respondents (46 percent) said their companies had a strategy in place for mitigating security risks posed by NGNs. This gulf between perceived need and actual implementation seems to confirm the ongoing trend of speed-to-market trumping security when it comes to rolling out new services.

As such, respondents indicated considerable concern over security of next generation services, including the following:

- *Only 2.5 percent believe initial IP-based television (IPTV) rollouts are “very secure.”*
- *About 92 percent said a hacker with “moderate” technical knowledge could compromise IPTV.*
- *Carriers consider mobile end-point compromise and core IP Multimedia Subsystem (IMS) compromise to be the greatest threats to NGNs.*
- *Almost 36 percent of respondents said security issues are impeding their rollout of triple- and quad-play service bundles (television, Internet, and fixed-line and wireless telephony).*

Ironically, respondents indicated that security is both a problem and an opportunity for carriers. As enterprises look to outsource more of their security functions, carriers view “in-the-cloud” security services to be a major opportunity for them. In fact, more than 80 percent indicated that in-the-cloud security services will be a major revenue generator within the next five years.

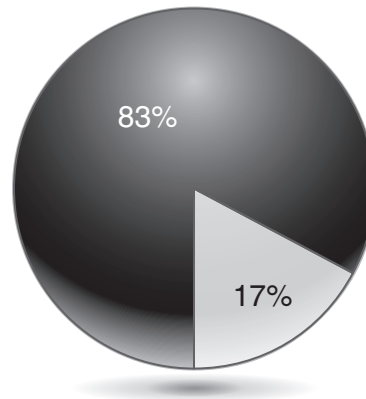
The following sections go into further detail on the survey responses.

Security and Service Rollout

Survey respondents continued to voice concern around security issues related to IP-based service rollouts. Following are specific responses to survey questions.

Question 1: How important is VoIP security to the long-term viability of VoIP services?

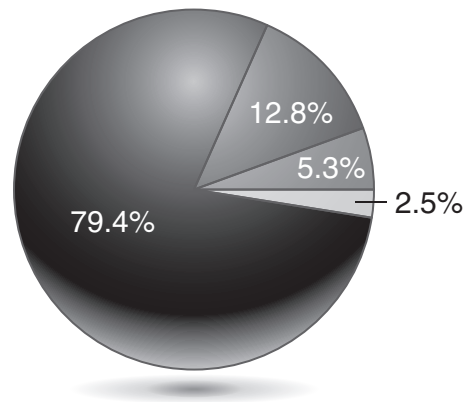
83 percent of respondents indicate that VoIP will fail as a service without strong security. The reason behind this is that it is easy for customers to retreat to “plain old telephone service” if they perceive VoIP as a threat vector. This remains relatively consistent with last year’s response of 78 percent.



- *83% of respondents felt that VoIP security is important to the long-term viability of VoIP services, and that VoIP will fail without strong security.*
- *17% of respondents felt that VoIP security is somewhat important to the long-term viability of VoIP services, and that if VoIP security is “good enough” it will succeed.*

Question 2: How secure are initial IPTV rollouts?

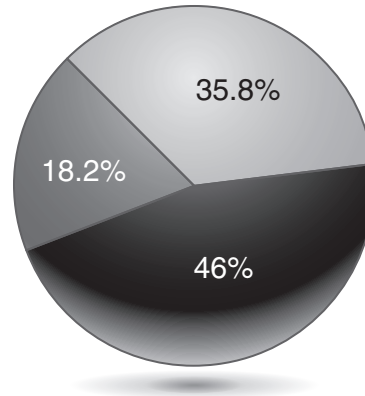
IPTV remains a source of security concern. Like most new services, in its formative stages the development focus on IPTV has been on delivering acceptable quality of service, rather than strong security. Thus, when asked about the security of initial IPTV rollouts, about 92 percent of respondents indicated that it does not require sophisticated technical knowledge to compromise IPTV. This represents a slight increase over last year, when 91 percent of respondents said they thought IPTV was either not secure or somewhat secure.



- 2.5% of respondents felt that initial IPTV rollouts are very secure, and it would take advanced technical knowledge to compromise IPTV.
- 79.4% of respondents felt that initial IPTV rollouts are somewhat secure, and someone with moderate technical knowledge could compromise IPTV.
- 12.8% of respondents felt that initial IPTV rollouts are not secure at all, and any garden-variety hacker could penetrate IPTV.
- 5.3% non-applicable.

Question 3: Are security issues impeding your rollout of triple- and quad-play bundles?

While triple- and quad-play services are becoming increasingly common, more than one-third of respondents (about 36 percent) said security concerns were impeding their rollout of these services. This is a significant improvement over last year, when 55 percent said security was impeding rollouts. This would indicate that carriers are overcoming some of the security issues surrounding the delivery of wireless and IP-based services into the home.

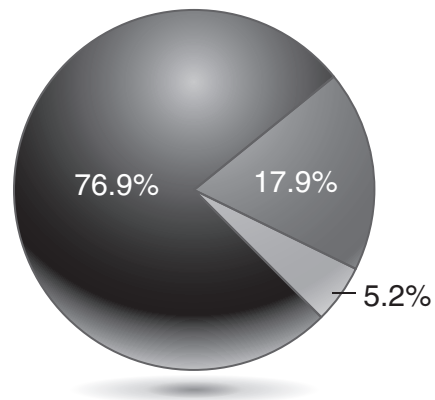


- 35.8% of respondents felt that security issues are impeding their rollout of Triple- and Quad-play bundles.
- 46% of respondents felt that security issues are not impeding their rollout of Triple- and Quad-play bundles.
- 18.2% non-applicable.

In-The-Cloud Security Services

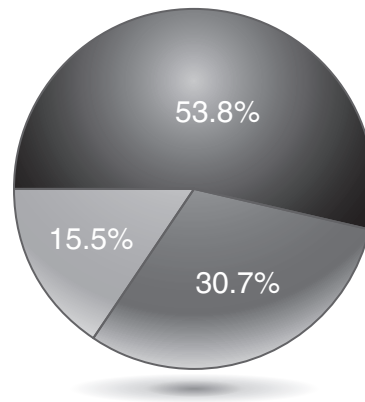
In-the-cloud security services continue to gain momentum with carriers. Nearly 77 percent of survey respondents said their companies have strategies in place for offering in-the-cloud security services. This represents a 13 percent increase over the 2006 survey. Additionally, while last year nearly half of survey respondents (49 percent) said they did not have the core competency to deliver in-the-cloud services, this year just under 31 percent said they lacked this core competency.

Question 4: Do you have a strategy for offering “in the cloud” security services to your customers?



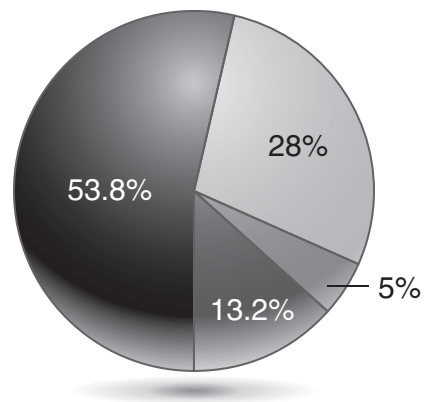
- *76.9% of respondents have a strategy for offering “in the cloud” security services to their customers.*
- *17.9% of respondents did not have a strategy for offering “in the cloud” security services to their customers.*
- *5.2% non-applicable.*

Question 5: Do you have the core competency to offer in-the-cloud security services today?



- *53.8% of respondents have the core competency to offer in-the-cloud security services today.*
- *30.7% of respondents do not have the core competency to offer in-the-cloud security services today.*
- *15.5 % non-applicable.*

Question 6: When do you think in-the-cloud security services will become a major revenue generator for your company?



- *53.8% of respondents think in-the-cloud security services will become a major revenue generator for their company within three years.*
- *28% of respondents think in-the-cloud security services will become a major revenue generator for their company within five years.*
- *5% of respondents think in-the-cloud security services will never become a major revenue generator for their company.*
- *13.2% non-applicable.*

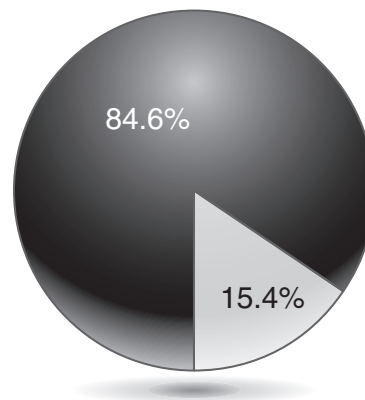
More than 80 percent of respondents said in-the-cloud services would be a major revenue generator for their company within five years.

Security and Next-Generation Networks

This year's survey also included questions specifically related to NGNs. As with the IP-based services cited earlier, survey respondents indicate that security has been a secondary consideration with the rollout of NGN infrastructure and services.

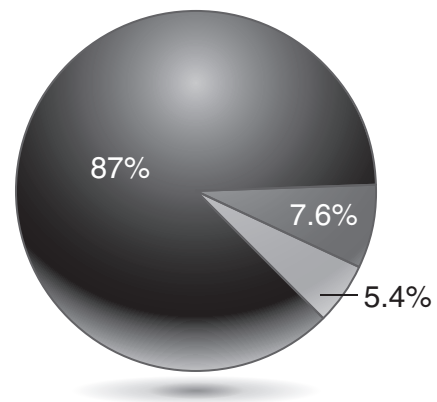
Question 7: Are you planning to roll out next generation, IP-based architecture in the next five years?

Two fundamental truths were revealed by the survey relative to NGNs: First, IP-based NGN architectures will soon be the de facto industry standard, with almost 85 percent of respondents planning to roll out next generation, IP-based architecture within the next five years. Second, security is critical to the ultimate success of NGNs, with 87 percent of respondents stating that NGNs will fail without strong security. However, it was also revealed that less than half of carriers (46 percent) have a security strategy in place to support IP-based NGNs.



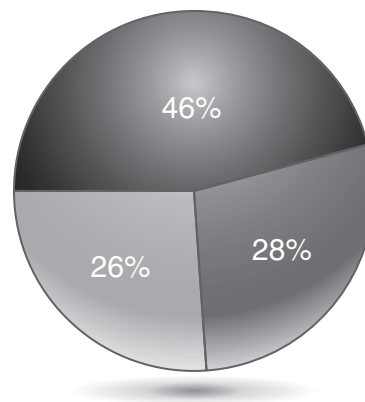
- *84.6% of respondents are planning to roll out next generation IP-based architecture in the next five years.*
- *15.4% of respondents are not planning to roll out next generation IP-based architecture in the next five years.*

Question 8: How important do you think security is to the long-term viability of next generation network (NGN) implementations?



- *87% of respondents felt security is very important, and NGNs will fail without strong security.*
- *7.6% of respondents felt security is somewhat important, and if NGNs' security is "good enough" it will succeed.*
- *5.4% non-applicable.*

Question 9: Do you have a strategy in place to support security risks posed by next generation, IP-based networks?



- *46% of respondents have a strategy in place to support security risks posed by next generation IP-based networks.*
- *28% of respondents do not have a strategy in place to support security risks posed by next generation IP-based networks.*
- *26% non-applicable.*

Question 10: In your opinion, what are the biggest security threats posed by next generation networks? Please rank the risks below:

(with “1” being the biggest security threat posed by next generation networks)

Rank:	Average Respondent Rank:
1. Mobile device endpoint compromise:	2.37
2. Core IMS network compromise:	2.4
3. IMS multimedia application threats:	3
4. Toll fraud:	3.6
5. Eavesdropping:	4.5
6. Location-based services:	4.7

Carriers view the customer as the most vulnerable point in their NGNs. Mobile device endpoint compromise was ranked as the no. 1 security risk, followed by core IP Multimedia Subsystem (IMS) network compromise.

Carriers and the Security Gap

The IBM Internet Security Systems 2007 survey of telecommunications carriers confirms that security remains a secondary consideration when carriers roll out new architectures and services. However, the results – particularly those around quad- and triple-play bundles – indicate that carriers will move quickly to address security issues once those services hit “mainstream” status.

The highly competitive marketplace is the driver behind this trend. Carriers are faced with the enormous challenge of reducing customer churn while introducing new revenue streams. New services help them accomplish both goals. However, this also places a premium on speed-to-market, which means they must first focus on developing services that provide high levels of quality and performance, often at the expense of security considerations.

However, the survey also indicates that security services represent a promising new revenue stream for carriers. As the rapidly evolving threat landscape outpaces the ability for companies to keep pace with their internal resources, carriers are well positioned to provide an outsourced security solution. This year’s survey showed a narrowing of the gap between the desire to offer in-the-cloud security solutions, and the presence of the core competency to do so. With more than 80 percent of respondents saying they expect in-the-cloud services to become a major revenue generator within five years, this gap should virtually disappear in the coming years.

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 preemptive protection for networks, desktops and servers. An established leader in security since 1994, the IBM Internet Security Systems 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 the IBM Internet Security Systems X-Force® research and development team – a world leader 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 IBM Internet Security Systems Web site at www.iss.net or call 1 800 776-2362.



© Copyright IBM Corporation 2007

IBM United States
IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America.
10-07
All Rights Reserved.


IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Internet Security Systems and X-Force are registered trademarks of Internet Security Systems, Inc. in the United States, other countries, or both. Internet Security Systems, Inc. is a wholly-owned subsidiary of International Business Machines Corporation.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

1 The IBM home page on the Internet can be found at **ibm.com**

 Printed in the (country of origin) on recycled paper containing 10% recovered post-consumer fiber.