

The Future of Telecoms Risk Management

An explanation of the changing nature of Risk in Next Generation Networks

A Præsidium Business Consultancy White Paper

APRIL 2011



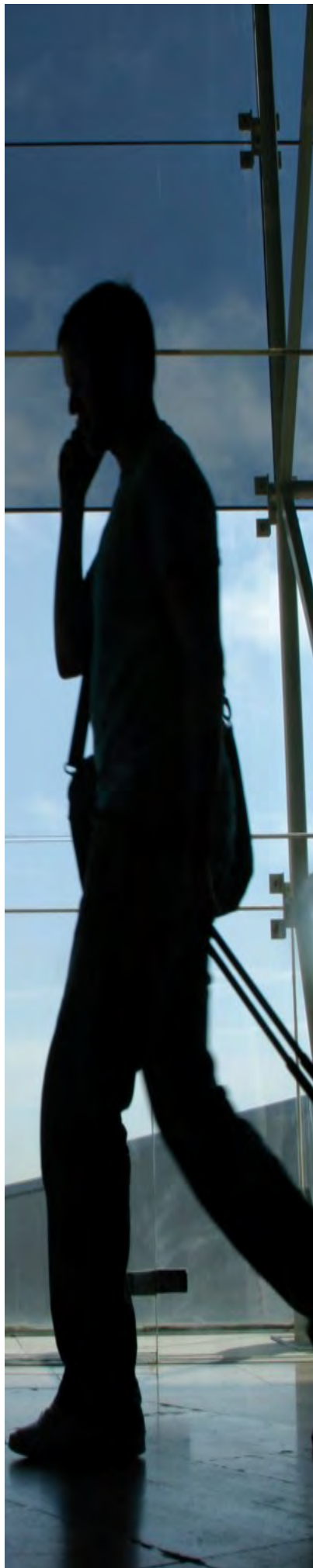


Table of Contents

New Risk Landscape for Communication Service Providers	3
Risk Management Identification and Control	4
Access Network Risks	5
Network Service Control Architecture	6
Data Capture	6
Service Provisioning	7
Identity Issues	7
Security Log Information	7
Fraud & Risk Types in NGN and IP Networks	8
Fraud Detection in NGN and IP Networks	9
Internet Abuse Management	10
Hidden Risk Management Concerns	10
Summary	11

1. New Risk Landscape for Communication Service Providers

For the last 100 years, the telecommunications industry has operated on the basis of providing both the communications channel (the bearer) and the content (the voice call). Next Generation Networks (NGN) being rapidly rolled out are creating the separation of services, whatever they are. The telecommunication bearer provides connection from the customer to the Communication Service Provider (CSP). Consequently, there are now a number of different players for the delivery of the services including:

- The CSP providing the connection from the customer to the service provider such as GSM, 3G, Wi-Fi, LTE. There can be multiple parties in the delivery of a service like a Wi-Fi network connected to a broadband network.
- The communications customer that owns the customer and controls their identity.
- The Service Provider (SP) that the customer uses such as VoIP, voice call, IP-Centrex provider.
- The Application Provider (AP) who supplies the download to the communication terminal device. These may or may not interoperate with service platforms provided by the SPs.

This all leads to a far more complicated service delivery path and increases the risks, due to the multiple players and inherent risks in both the service and bearer delivery models.

“The introduction of Next Generation Networks means the services and bearers are separate and can be operated by different players”

This has been coupled with a decrease in revenue from traditional streams such as voice and a large increase in competition. To maintain profitability, CSPs and network operators have been rolling out new offerings using data services and improving the end user applications and experience.

In addition to the significant change in the way new services are delivered, there is a rapid change-out of network equipment due to pressures forcing CSPs to improve efficiency and reduce cost, including:

- Reducing the upgrade cost of its infrastructure
- Lowering the cost of staffing for operation and control
- Reducing power consumption and operating costs

While these are all very significant items in their own right, CSPs have taken the view that their core skills are not in network operations, but in providing the acquisition of customers and providing them services. Based on this, many are moving to an outsourced model for the supply and operation of

the bearer and in some cases the supporting services network.

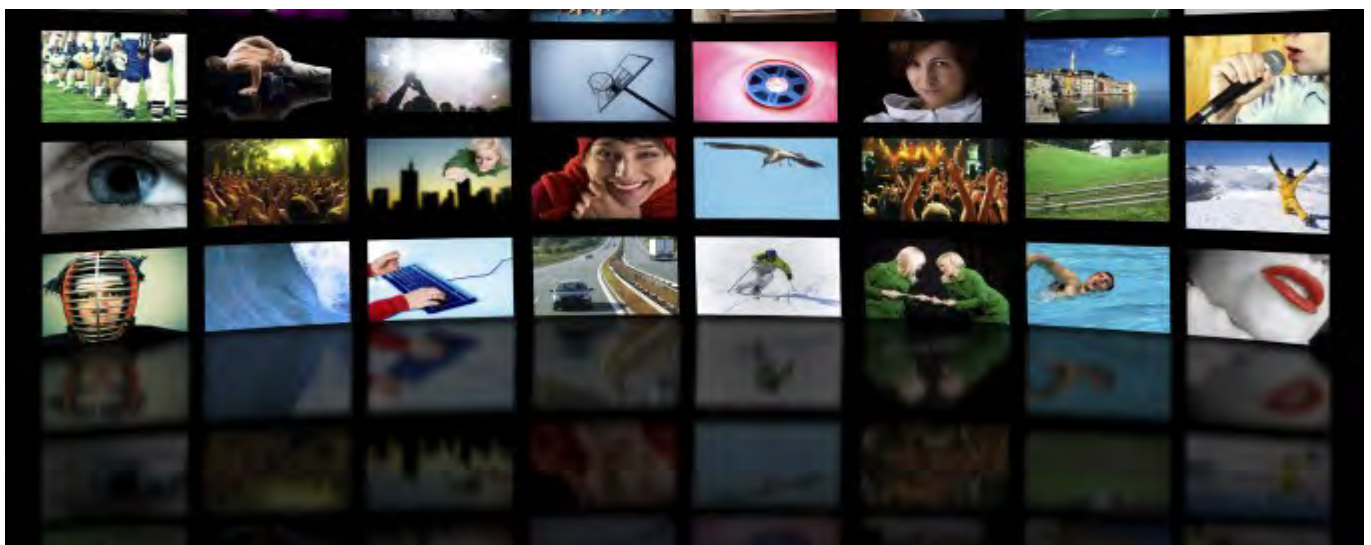
This means many of the risks are outsourced from a technical and operational aspect. However, without the control that a CSP can apply they retain the risk without it being transferred to the outsourced partner.

“CSPs are rapidly changing out old circuit switched technology to new IP based communications systems but there is little risk manager experience for these new systems”

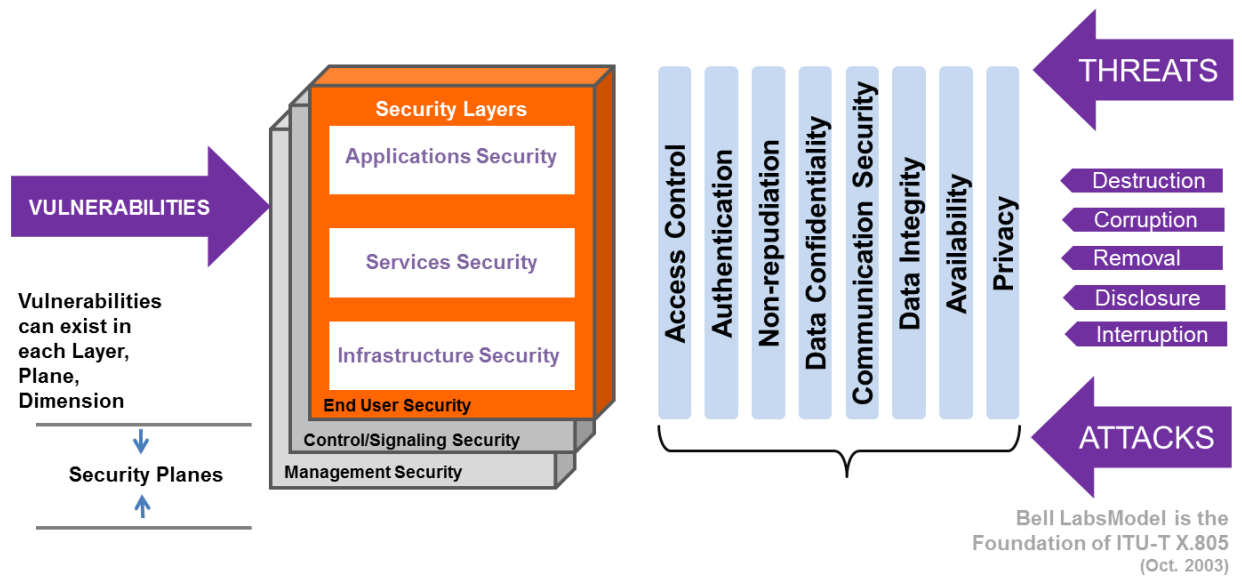
According to some industry research reports, “87% of survey participants indicated that Next Generation Networks will fail without strong security, however fewer than half of the respondents (46%) stated their companies did not have any strategy in place for mitigating Security Risks of any type posed by IP NGNs.”

It is evident from the client projects Præsidium has delivered, that the understanding and planning for NGN in the areas of risk and fraud control is very limited.

(1) IBM survey



X.805: A Model for Evaluating End-to-End Communications Systems



A holistic system-level security thought process is essential

- Organize amazing complexity into bite-sized requirements
- Common approach leads to shared understanding
- Standardization essential to interoperability in multi-vendor networks

2. Risk Management Identification and Control

The challenge of assuring risk management is often an activity spread across a number of sectors within a business including: Fraud Management, Revenue Assurance, Internal Audit, IT Security and Network Security. With the changing landscape, many CSPs do not have a clearly defined strategy or view of the risks involved and assume they are not as risk prone as they may have been in the past.

“While standards are good at providing general controls and do limit some risks, they often give a false impression of risk control”

In reality, most CSPs are now more likely to have inherent risks in their network and be exposed to high levels of abuse and fraud of a more technical nature.

To address these challenges, CSPs need to implement a holistic risk management strategy employing professionals that are thinking from a risk management perspective. This is often contrary to the normal business process, as these professionals have to think more like a “criminal” to identify the risks.

To assist in the risk management process, companies use different industry standards and frameworks. Often they believe that if they have implemented ISO9001/2 or 27001/2 they have covered the security risks. While these standards are effective for providing general controls and do limit exposure to some risks such as making a business think about disaster recovery, they do not cover risks caused by the customer or criminal element.

In Præsidium’s experience, the use of modified end to end risk management models provides a stronger and more robust control framework. As an evolution of this, Præsidium uses a modified version of the ITU X805 standard with some of this now being

incorporated into ISO 27011 (specific security standard tailored for CSPs)

This method provides an end to end holistic view of security risks and provides a methodology to ensure that the services used by the customer are reviewed throughout the business ensuring risk minimization.

“In Præsidium’s experience, there are always significant risks in the access network configuration. Even latent security risk issues that are over 10 years old may still not be resolved”



3. Access Network Risks

There are many network types in use today, but the majority of these are related to IP services built on the 3 key areas of Mobile, Broadband ADSL and Cable. In addition, there are many other access methods including; Wi-Fi, WiMax, LTE and NFC. All of these access methods present different security risks that are compounded when multiple access methods are used.

While many CSPs understand the risk of their main network technology type, many are now either buying capacity on other network types or buying complete new networks of which they do not have the same level of experience or expertise. Added to this, the network may now not be controlled by the CSPs staff and so they are relying on the vendors to support the network.

There are always significant risks in the access network configuration. Even latent security risk issues that are over 10 years old may still not be resolved. These are often in the area of customer authentication for the protection of the communications traffic from the customer terminal to the

network.

The risks in the access networks are often exploited for criminal gain, or for causing abuse to the CSP such as theft of the service from the customer. NGN will often still rely on the access network to provide protection from theft and abuse so while new network security nodes may be added, such as a RADIUS or AAA server, risk mitigation is still essential in the access networks.

Assessing and understanding the access network risks are therefore essential and CSPs need to consider exactly what is being defined.

“IMS and similar service enabling architectures mean that it’s simpler to integrate different network types but also bring a group of different risks together”

4. Network Service Control Architecture

CSPs are changing the way they operate with a drive to allowing multiple access networks providing simplicity and speed of deployment of applications that use control framework architectures. The one specified by ETSI and 3GPP is the use of the IP Multimedia Subsystem (IMS), although other types exist. They allow the access network to communicate in a standardised way to a number of different elements such as subscription databases (HSS), application servers, a mobile switching server (MSS) or session border gateways and media gateways used to interface to other networks or services.

IMS is an architectural framework, originally designed by the wireless standards body 3GPP. It is used for delivering IP multimedia services to end users and was part of the vision for evolving mobile networks beyond GSM. It has now been updated to include migration and convergence of the other access bearers, for both mobile and fixed NGN platforms. The premise was that, where possible, it would use Internet standards and protocols such as SIP. The intention of IMS is not to standardise applications, but to aid the access of multimedia and voice applications across mobile and fixed terminals. A major element of IMS design is that it provides horizontal control layers that isolate the access network from the service layer. Each service does not have to have its own control functions as the control layer is a common horizontal layer. As it is an enabling technology, it is difficult to specify the fraud and security controls, as it will depend on the access provided and services carried rather than the transport layer.

IMS provides the ability to have 'integrated services', which are independent of the access method and potentially also independent of the network operator. This integrated services approach can provide benefits to the collection of information for the purposes of fraud and risk control.

IMS enabled terminals need to be able to handle the IP and IMS connections and the associated protocols and new identities used. In traditional networks, the identities used are relatively simple and are in principle fixed for the customer (either a fixed directory number, MSISDN or IMSI in GSM mobile etc.). With IMS, there are several new identities, for example: IP Multimedia Private Identity (IMPI) and IP Multimedia Public Identity (IMPU). Both of these are not phone numbers or other series of digits, but are URIs (Uniform Resources Identifiers). Numbering can also be different; this is performed using ENUM DNS, which is set up to allow movement of numbering between the IP and PSTN worlds and to enable security to make changes to the routing (call forwarding, transfer etc.).

The identities and numbering that are used can be dynamic and are, therefore, harder to understand for

a fraud or risk analyst. The risk management system will need to manage multiple identities in a logical way. At present, there is generally one account for the customer who owns and uses the service, but this will not necessarily be the case in an IMS network, as different accounts for different services could be used and operated.

5. Data Capture

The way information is collected from access networks, the core network and IP and IMS services is, in principle, similar to the approach currently used for Fraud Management and Revenue Assurance Systems. It can be collected from network platforms, mediation systems, billing and more importantly the signalling systems. In many NGN architectures there are additional mediation or event record billing platforms such as the Ericsson EMM.

With signalling information, the volume of information collected is far more complex than for existing FMS or conventional risk management systems. Many conventional systems will not be able to cope with the changes that need to be made to handle the variety of data. For example, the signalling used in VoIP, IP and IMS typically use SIP and DIAMETER signalling which is very different to SS7 formats. The points of collection selected for IP and IMS fraud control will depend on the configuration of the network, the extent to which the fraud or risk detection of the service is performed and the specific CSP requirements and capabilities of its BSS/OSS platforms.

There are now specific fraud and risk management tools that interface solely with the network signalling and with good reason. This is fundamentally the most accurate point to monitor customer activity and event types of the service offerings. The data used is now more complex than ever and the collection of this data is challenging. However, the introduction of new network elements such as the SBC can offer rich IP session based information for fraud and risk management purposes. With this in mind, many CSPs are now reviewing and planning the way forward for NGN and service based fraud management.





6. Service Provisioning

The changing landscape for CSPs, coupled with the customer's expectation that voice calls are very low cost or even free will mean that more and more services will be based on a monthly flat fee for items such as broadband access, VoIP and IPTV, Skype, local call plans etc. This creates the need to develop 'provisioning-based' fraud and risk detection that can be seen as either a revenue assurance or fraud control activity and depending on the company, either model may exist. This issue is compounded by the fact that many NGN services are being self-provisioned such as 'iTunes'.

Provisioning based fraud detection is equivalent to the present concept of looking for ghost subscribers in the fraud system. However, this concept has to be extended to the service layers as well as the access bearer layers. Fraud detection will need to identify the use of services that are not provisioned for a particular customer.

Unlike today, where all information is either in the billing and customer care systems or the IN platforms for prepaid, in the IP/IMS converged network, there will need to be a common service profile for the subscribers. This would include the service and bearer component from the fixed, mobile or other access environments. In a fully IMS environment, the HSS containing user specific details such as identities and service profiles are held in the SRD unlike in GSM where customer data is stored in the HLR. For many years to come, there will be a mix of infrastructure and hence of identities. Consequently, service profiles will be in several locations adding to the complexity and risk for CSPs and customers.

"Provisioning based fraud and risk detection becomes vital in a converged and self-care network"

7. Identity Issues

There are a number of identities used in NGN, IP and IMS networks. The integrating of these identities will be a key part of linking the services and access layer networks where they are separated. The information can be static or dynamic, therefore mapping the identities together will be vital. CSPs will need to provide one common resource that automatically links information from the different service layers to the bearer layers and account level.

Items to be mapped between systems can be stored either in the network database of the FMS/ Risk management platforms or in the feeder system that is handling the signalling requests at that time. This would be similar to today, where an enquiry of the billing system and HLR/AuC can be made to verify customer details and payment information.

8. Security Log Information

With the integration and risks associated with IT security and both the services and bearer layers in telecoms being IP based, the use of an IT security system is seen as a potential source of information for fraud and risk management.

Firewalls, log servers, syslog servers, routers etc. can be used to collect valuable information. However, the collection devices are generally configured to have limited event logging due to the loads on the devices themselves and the services passing through them. There is potential for significant useful data to come from these devices, with most of it being related to events from different forms of attack or connection activity.

Security management systems have not been designed, in most cases, for Fraud or Risk management purposes, but they can be used to generate alerts on the identities detected that are involved in security incidences in the associated IT security systems. It would not be economic to replicate the security monitoring functions of logging systems in an FMS, but alerts could be used as inputs to the FMS and applied to the rules and business logic of such systems.



9. Fraud & Risk Types in NGN and IP Networks

The general risks of IP based Telco systems are a mix of those witnessed from the Internet and also have the same characteristics as telecoms specific risks. The convergence of services brings convergence of risks, therefore the tools CSPs use to combat these risks will have to evolve. While a traditional FMS can cover some aspects, new types of fraud and risk types will need to be managed. These will include items such as:

- IP/identity spoofing
- Access bearer theft
- Denial of service attacks
- Virus or Malware
- Over-billing attacks
- Reselling of content services
- SPIT (Spam over Internet Telephony)
- Unauthorised access to VoIP, IP Centrex, or other services.
- SS7, SIP, H323 Protocol Abuse
- Eavesdropping of content transferred
- Excessive downloads
- Use of rogue IP diallers used to generate false traffic
- Theft or abuse to streaming content such as video stream.
- Customer identification and vendor identification manipulation
- Illegal interception
- Manipulation of content platform and gateways
- Attacks on payment gateways
- Stored data capture theft in application servers

The level and type of fraud experienced by CSPs will be based on the charging method for the bearer, services, payment or content offered, which will be dictated by the specific commercial arrangements of that CSP. There will be a general shift from payment for the level of use of services, particularly for voice calls, SMS and data consumption to a system of

single flat fees for use upto certain limits. There will be a greater focus on provisioning assurance of both the bearers and services offered. Strong credit management policies and provisioning fraud detection will be critical in this environment.

“The charging method for the bearer and services dictate the frauds and risks prevalent”



10. Fraud Detection in NGN and IP

“The fraud profiling and rules engines will need to work in a combined way on not only the services offered, but also on the bearers used”

Rules used in fraud management for NGN, IP and IMS are, in principle, the same as those currently used but with new and complex relationships due to the new data types and data sources involved. The same combinational logic will be needed for rule building, where the FMS will require the ability to implement rules that are based on a combination of:

- Network event records (from mediation, billing or built from signalling messages)
- Session border gateway data
- Multiple identities – using look-up tables or making enquiries of other platforms such as HSS
- External alerts from security monitoring systems
- Customers’ services profile information
- Any piece of data imported to the FMS for flexible rule creation e.g. from content gateways

As outlined, there are now more risks that need to be controlled, and detected particularly from a provisioning and credit monitoring perspective, as

well as the existing fraud detection conducted. The key areas for such systems will include:

- Linking of services and bearer layers identities and identity management.
- The need to profile the use of services for each individual subscriber. This is unlike today, when it is assumed that people have the right to use the services and where the extent of use is reviewed for fraud management purposes.
- The need to monitor different origination and termination identity types. These are generally linked today to one account identifier, but in the IP/IMS world, their display and management will need to show other identities.

IP based fraud detection will focus on ‘provisioning-related fraud’, with the FMS needing to know which services the customer is allowed to use. There are numerous generic types of IP services that require monitoring, including:

- Voice-based (VoIP, IP Centrex, IMT)
- Message-based (SMS MMS)
- Streaming-based (IPTV, VoD)
- Interactive (e.g. ‘Second Life’ gaming, Social networks)
- Content-based (downloads of applications and games downloads)
- Subscription-based (e.g. location services, IM, presence indication)
- Pay-per-Push.

“The charging method for the bearer and risk are similar to today but the combination of more complex and significantly more data makes risk management a challenge”

11. Internet Abuse Management

Most mobile operators have now ventured into the world of mobile Internet even if it is still only seen as a VAS and not a mainstream product. Unfortunately, this makes them, even on a small scale, an Internet Service Provider (ISP) and most have not considered the corporate responsibility, legalities or regulatory requirements.

Some consider the regulatory requirements (for example, Web site filtering for child pornography) but few consider the corporate responsibility of controlling their services from being used by Spammers or hosting internet fraudsters.

So why should a CSP consider implementing the controls normally associated with an ISP? Well, in NGN IP based networks there is an ever reliance on data and internet connectivity in the delivery of services. This is further compounded by the rapid take up of mobile Internet dongles and embedded machine to machine (M2M) devices, meaning that the operating model is more of an ISP with similar resulting abuse and control problems. The effect of the changes and the introduction of high speed broadband enable Smartphones and Tablet devices to have multi-access high speed network enabled devices.

Managing this type of traffic for fraud and risk, changes the landscape for CSPs. They cannot now monitor and control every event, but are looking for fingerprints or traffic profiles. The use of flat rated billing models often means the CSP will not be interested where the traffic is destined, so long as it does not affect the overall quality of the customer experience. This has implications for fraud management and makes the task more difficult. Add the anonymity of prepaid service and this creates the perfect environment for an internet abuser to operate with very little policing.

The complexity of mobile internet makes it difficult to identify a customer when they have accessed an Internet site. Customers are given an internal dynamically allocated IP address each time the customer creates a session (or connection to the GGSN). This means that over a period of time, depending on the IP address recycling process, many different customers will have used the same IP address identity. Couple this with the fact that as the connection passes on to the Internet, the firewall will translate the internal IP address to one recognised in the Internet world. So when a customer accesses a website, the CSP's external IP address is registered.

The *Wikileaks saga* has highlighted how effective 'hacktivism' and the social networking era can be. 'Operation Payback' run by Wikileaks supporters demonstrates just how quickly large, disparate groups can organize and with relatively simple technology, do very real and significant damage.

In the same way that there is a potential loss of control of IP identity in mobile networks, email has similar issues as it travels through an SMTP proxy to keep internal and external connections apart. So any email sent from a customer will look like it comes from the same email proxy. If they generate email SPAM using this connection, then other ISPs and email service providers will blacklist the IP address of the offending proxy, thereby stopping all customer email. This is fine if it is a little known service, but what about Yahoo or Hotmail? This has happened to some larger CSPs and affected millions of customers. When CSPs register for a range of IP addresses, they are required to provide a publically available email where anyone can contact them. On this account, items worthy of analysis and control measures include:

- Copyright infringement
- Internet fraud
- SPAM detection/monitoring
- Denial of services attacks (as witnessed with the Wikileaks attacks)

“While fraud is seen as an issue, internet related abuse affecting CSPs will increase and will cause an ever increasing problem on the operations and reputation of the CSP”

As a CSP that just maintains a 'bit pipe', it has no control or responsibility over what the customer does (this has always been the case) but in the case of abuse and fraud against others, unfortunately it is only the CSPs IP address that can be used as the offending identity. Therefore, the CSP must be able to control and monitor the customer to prevent other parties that may be affected from being blocked or blacklisted. To control these risks, the CSP needs to:

- Find out who owns and monitors the registered email address and have them verified
- Obtain supporting information as part of the enrolment process
- Ensure the CSP clearly understands the Internet regulatory requirements of its own country but also of the interconnection points and peering links

12. Hidden Risk Management Concerns

A key aspect for CSPs over the years has been changing operational processes due to their size and complexity. In doing so, they have lost the full end to end understanding of the business. When it comes to risk management and fraud, the whole end to end process is critical. In Præsidium's experience, many business risks are due to this lack of end to end understanding of the service, platforms and processes. During CSP review programs, Præsidium has identified that there are hidden risks between departments and between different systems. This is further compounded if the network is set up or configured by the equipment vendor who often has little interest in performing a full risk review as they are not accountable for any risks or frauds.

Another problematic area is that there is often a significant lack of understanding of the current and historic network configuration. This is typified in discussions with managers who have been operationally "hands on" involved in the past and have then been promoted. Their understanding of the issues are based on a previous time and in a fast moving business, the network configuration settings and services are rapidly changing. This issue creates a gap along the whole of the service chain.

A review of the service chain is vital to understand the actual configuration and that expected by management and staff. This is best accomplished using a strategic risk review against recognized methodologies by qualified staff that have the necessary domain level expertise. This review should be followed by further in depth analysis in key risk and fraud areas to ensure the mitigation of risks can be implemented. Following this key activity, the CSP should ensure that a set of control frameworks and policy & procedures covering risk management are implemented to track and control the likely introduction of risk.

While this initial investment can be high considering the time and effort required from the CSP, the Return on Investment is significant due to the mitigation of losses. A single concerted fraud incident can exceed €100k, more than the cost of an initial review and the first year's implementation of control activities. Typically payback can be 1 to 2 months, if not less.



Summary

The risks for CSPs in a converging telecoms market moving to a NGN environment based on a fully IP based communication and control system are significant. CSPs that are changing out their entire network or significantly upgrading to fully IP, need to consider the longer term risk management strategy. This needs to be based on:

- Ensuring the organisation is able to understand and manage NGN risks
- Determining a baseline of the current position in regard to risk and fraud control by performing a strategic risk review
- Creating a risk register covering the current and expected mitigating controls
- Developing clearly defined control frameworks
- Implementing the necessary policies and procedures for the measurement and management of risk & fraud control

While the tasks for many CSPs may be recognized, there is often a lack of internal understanding of the many hidden risks. The task may seem very large and complex, but Præsidium is able to offer its expert industry leading support in the complex world of risk management for NGN/IP communications networks. Præsidium's expertise and industry experience, coupled with its proven risk management methodologies can successfully complete the necessary risk evaluations in weeks, where as a CSP may take years. This cost effective approach to identifying and mitigating risks is evident in the growing list of CSPs that have commissioned Præsidium's consultancy expert support in this field.

Glossary

AS	Application Server
BFM	Bearer Fraud Management
CSCF	Call Service Control Function
HSS	Home Subscriber Server
IAD	Integrated Access Device
IDS	Intrusion Detection System
IMS	IP Multimedia Subsystem (3GPP standard)
MGCF	Media Gateway Control Function
OFDM	Orthogonal Frequency Division Multiplexing
PFM	Provisioning Fraud Management
PPPoE	Point to Point Protocol over Ethernet
PVC	Permanent Virtual Circuit
SBG	Session Border Gateway
SFM	Services Fraud Management
SIP	Session Initiation Protocol
SRD	Service Resources Database

About Præsidium

Præsidium is a Global Business Assurance consultancy.

Founded in 1997, the company has successfully provided risk management consultancy to more than 100 Communication Service Providers in over 80 countries on 6 continents. Præsidium has gained solid recognition in the market amongst its substantial customer base and among global standards agencies. These include the GSMA Security Group & Fraud Forum, the Telemanagement Forum and ETSI.

Offices:

United Kingdom
Davidson House, Forbury Square,
Reading, RG1 3EU,
Tel: +44 118 900 1054
Fax: +44 118 900 1055

Brazil

Torre Rio Sul, Rua Lauro Muller 116;
27º Andar – Sala 2701
CEP: 22299-900 Botafogo
Rio de Janeiro
Tel: +55 21 2543-5419
Fax: +55 21 2543-5419

Ireland

Maple House, Temple Road, Blackrock,
Co. Dublin
Tel: + 353 (0)1 400 3900
Fax: + 353 (0)1 400 3901

Portugal

Edifício Picoas Plaza
Rua do Viriato, 13E núcleo 6 - 4º andar
1050-233 Lisbon
Tel: + 351 210 111 400
Fax: + 351 210 111 401

Spain

Edificio Cuzco IV
Paseo de la Castellana, 141 8ª planta
28046 Madrid
Tel: + 34 91 572 6400
Fax: + 34 91 572 6641

USA

3333 Warrenville Rd.
Suite 200
Lisle, IL 60532
Tel: +1 630 799 8081
Fax: +1 630 799 8083

On the Web www.praesidium.com

General Information info@praesidium.com

About WeDo Technologies

WeDo Technologies is the number one preferred supplier for revenue and business assurance software and services.

Present in 15 countries on 5 continents, with more than 100 innovative bluechip customers in more than 70 countries, the company has a solid and enviable project management track record of being on-time and within budget while achieving superior customer satisfaction.

Business Assurance RAID®, WeDo Technologies' flagship software suite covering Revenue Assurance, Fraud Management and Business Processes Control has been implemented in a number of different industries where it has delivered significant business results and powerful return on investment. WeDo Technologies pioneered the telecom revenue assurance space in 2002 and is now breaking new ground in the enlarged business assurance arena in Telecom, while also servicing the Retail, Energy and Finance industries.

Offices:

Portugal _ Lisbon

Portugal _ Braga

Australia _ Sydney

Brazil _ Rio Janeiro

Brazil _ Florianopolis

Chile _ Santiago

Egypt _ Cairo

France _ Paris

Ireland _ Dublin

Malaysia _ Kuala Lumpur

Mexico _ Mexico City

Panama _ Panama City

Poland _ Poznan

Poland _ Warsaw

Singapore _ Singapore

Spain _ Madrid

Spain _ Barcelona

UK _ Reading

USA _ Chicago

On the Web www.wedotechnologies.com

General Information customerservices@wedotechnologies.com