XINTEC
THE WORLD'S SMARTEST RA TECHNOLOGY

HELPING SMALLER CSP'S **OVERCOME THE CHALLENGES** IN EFFECTIVE RISK MANAGEMENT

Xintec understands that smaller CSP's have the same operational concerns in respect of fraud and revenue assurance as the larger tier one operators.

However, for smaller operators there are some quite different challenges they must face to achieve their desired outcomes in these areas. These challenges include operational resource availability, infrastructure, finance and capability which all impact the results that can be achieved by Fraud and Revenue Assurance (RA) teams within the smaller CSP.

Frequently smaller operators fall into the trap of not recognising the importance of fraud and RA systems, or t ry and create in house solut ions, often leading to increased financial losses when incidents do occur.

THE FRAUD IMPACT FOR SMALLER CSP'S

Recent surveys on fraud such as the CFCA fraud loss survey (2011) highlight how fraud is still a major issue for CSP's with 89% of the respondents stating that fraud losses had increased or stayed the same within their own organizations year on year. The headline figure for the industry extrapolated from the results of the survey show an average estimated loss of 1.88% of revenue to fraud.

However the percentage loss for smaller CSP's will in many cases be much higher than this, as that average figure is lowered by the influence of the major tier one European and US carriers, who make significant investment on fraud management tools and resources, so can maintain fraud losses below 0.25% of revenue on an annual basis.

Many smaller tier 2 and 3 CSP's, new entrants and those in emerging markets have reported losses of between 4-6% of revenues from fraud, figures which can have a significant impact on a smaller CSP trying to maximise profits and their growth potential. It is known that Fraudsters will often target smaller CSP's, knowing that their internal resources, processes and fraud detection systems are generally not as robust and effective as in most larger operators, and consequently allowing fraudu lent activity to continue longer to maximise their profits.

Reported fraud incidents consistently show that even over short time periods, these events can result in losses of hundreds of thousands, or in extreme cases, millions of dollars to a CSP. While fraud losses at this level are significant for any CSP, many larger Tier 1 operators can manage the impact of them, however an incident on a similar scale targeting a small CSP is likely to resu lt in a more serious financial impact, sometimes taking years to recover from.

Examples of some of the current top fraud threats:

- International Revenue Share Fraud (IRSF)
- Bypass (or Simbox)

INTERNATIONAL REVENUE SHARE FRAUD (IRSF)

A recent survey by the GSM Association Fraud Forum into IRSF, confirmed that this fraud was a major concern to all operators who responded. Although the survey found that IRSF was not the most common fraud being experienced by CSP's, it did have a greater financial impact per event than any other fraud. The survey also found that IRSF was particularly prominent in highly competitive markets where fraud controls were often sacrificed using the argument that this made them more competitive and stimulated growth, placing a greater need on effective fraud detection systems.

"A UK Tier 1 Mobile operator lost S 1.2m to IRSF in one month in 2011 and overall $4.5m over a six month period." Mobile news 2011

BYPASS (OR SIMBOX)

This service abuse has been consistently highlighted in the top three fraud types being experienced by CSP's for the past severa l years (CFCA/GSMA). This type of attack is particularly prevalent in growing emerging markets where there is increased competition combined with high interconnect termination charges.

"An African Mobile operator lost over $9million to Simbox activity in 7 months during 2011. All other operators within this Country also experienced significant losses to Simbox activity." Juniper Report 2012

Implementing a system to manage revenue risk should be a priority for any CSP, however there are many issues and challenges that must be considered in order to ensure that any system implemented is fit for purpose in respect of the specific requirements of the CSP involved. The focus must be to do this effectively and efficiently in order to gain the best result for the organisation.

THE CHALLENGES - HOW XINTEC ENABLES YOU TO COMPETE

The First Challenge - Finances

Traditional fraud systems have historically been designed with large scale tier one operations in mind for large database and complex network infrastructures and as such are normally expensive, difficult to install and maintain and requiring resource intensive support.

Smaller CSP's do not generally have the infrastructure, resource or available skills sets to manage such solutions, and although scaled down options are being made available; these often still have high total cost of ownership (TCO) impacts.

XINTEC recognised this, and have addressed the issue by designing solutions ta ilor made for the smaller CSP, removing the need for high cost infrastructure and support systems without compromising on detection and prevention techniques and methodologies.

We understand that smaller operators have a greater risk exposure, more specifically related to impact, and have a greater need to optimise cost

and operational structures. XINTEC's solutions provide fast and efficient ROI combined with a lowTCO to ensure the CSP gains maximum benefit from the investment.

Total cost of Ownership is a very important factor to be considered for any system implementation, particularly for a smaller operator - gaining true value from a system implementation is essential.

Taking a cut down version of a system designed for a greater level of infrastructure and support can impede cost effectiveness in the long term. The design of XINTEC's solutions for fraud and RA means that there are no expensive additional costs borne out over the lifetime of the product for components such as the database and other third party software.

The Second Challenge - Operations

Establishing an effective and efficient fraud operation within a small operator can be a challenging task. Small operations tend to be restricted in the number of resources being made available and often lack sufficient skilled expertise in the fraud and revenue assurance area. Without access to fundamental knowledge of the Telco operational architecture, data structures, services and operational threats, it is almost impossible to implement the effective operational infrastructure to provide adequate protection against fraud.

Many organisations however do not have time to develop staff into these roles or cannot obtain experienced personnel with the required ski ll sets with the limited budgets available. Often smaller operators in these situations tend to establish fraud management or revenue assurance operations based on their limited knowledge or experience in these areas, which can resu lt in a focus only on issues previously experienced, and supported by ineffective in house created reporting systems. Due to the constantly changing technology environment we work in, our industry risk profile is changing almost month on month, so many of the outdated and manual approaches to revenue risk management are simply no longer practical. Similarly, many in-house developed systems which may have been 'fit for purpose' for specific revenue risk management issues when implemented, will have become difficult to maintain and adapt to today's constantly changing risk environment. XINTEC has created a solution suite to meet these operational constraints, utilising their industry knowledge and experience of telecommunication risk management for the smaller CSP. The XINTEC solutions are rich analytical tools that can be utilised quickly and effectively via intuitive interfaces.

A modular based architecture allows the CSP to utilise what they need for the services they have active, with the ability to grow and expand preventing operational stagnation.

The solutions also contain preconfigured built in controls for the main threats to services that could be experienced by a CSP. These controls can be adjusted and managed by the end user as knowledge and experience is gained, their risk

profile changes or as built in profiles develop. This allows the system to deliver immediate value from the day it is implemented then on allowing the user to optimise operational efficiency in the day to day operation as their experience grows over time.

By providing user friendly and preconfigured modular options, the XINTEC solutions suite allows the CSP to quickly establish an operational risk detection and management function. Inbuilt system risk detection methodology can, with minimal experience, be finetuned by the CSP analysts to improve effectiveness and efficiency.

The Third Challenge-Technology

The issue of technical architecture is one of the biggest challenges for small operators wanting to establish effective risk management practices.

Advancing technology in a competitive marketplacecan present obvious difficulties for smaller operations competing with the larger providers, but it also presents an internal challenge in establishing optimal operations.

As mentioned previously the traditional risk management system vendors created their solution architecture with large tier one operators in mind.

These operators would have specialist components that would support any system implementation. Vast technical support, along with implementation and project resources would normally be available to support any project during the lifecycle of the solution.

Risk teams would have multiple resources to manage each step of the process and be able to deal with the complexity of the solutions.

Therefore these systems would have significant technical requirements, such as large data warehouses, significant hardware, technical support teams, configuration and coding specialists etc.

The solutions would also be configured with multiple products, services and markets in mind utilising an array of combinations of analytics to perform the same task in multiple ways.

However - for the smaller operator many of these specifications are redundant. Mass resources to support such implementations are not available, cost and scale restraints tend to drive streamlined service and network infrastructures, whereas product and service capabilities tend to be more focussed or compressed to drive customer value and profitability.

Therefore a leaner more scalable approach is required in order to provide smaller CSP's with value from investment in risk solutions.

XINTEC have created a solution to ensure that the issues for smaller operators are addressed and do not impede the ability to perform.

Our solutions are created specifically to exclude the requirement for the large technical infrastructures of traditional systems. Aspects such as open source database solutions remove the need for expensive large database solutions and other such third party components, only XINTEC software is required.

Modular components allow focus on only relevant products and services and the related risks, this also ensures that only the hardware architecture is utilised to perform the task in hand, and not support multiple processes that have no relevance.

Pre-configuration and simple to use management tools avoid high level technical expertise for support and operation.

The Fourth Challenge- Functional Capabilities

The Final hurdle to be progressed for any small operator looking to implement a risk management operation and solution is that of capabilities.

If the CSP decides to self-build an operational solution capability, this is where the size and scale of the operation can seriously impede any effectiveness. Finding the appropriate resource internally to create and manage any reporting or alerting infrastructure is difficult, especially with clashes of priorities and responsibilities. Even in situations where this resource is available, development of the appropriate controls, monitoring or reporting can be limited due to lack of knowledge of the issues or understanding of the mechanisms needed to achieve the goal.

Even if an operator does manage to establish a simple self-built control or reporting system, the lifecycle of such a system is limited, as risks change and develop over time and constant management and updating of such solutions are needed.

So what about the traditional solution providers?

As these solutions have been built with large operations in mind, they are usually highly complex systems, with multiple capabilities embedded into their architecture and are designed around the large scale operator process, which can be much more complex and intricate then necessary.

It is often found that where small operators have implemented such solutions that a large percentage of the functionality is actually redundant in terms of the day to day needs of a smaller operator, this combined with the added complexity often included in the analysis and decision making process usually means that the end user in the smaller operator is overwhelmed and consequently inefficient.

At XINTEC, we believe a CSP should not be impacted on performance or capability by having a third party risk management solution. Our software has been created to be flexible and powerful at the same time.

Created as a building block modular architecture, it enables a CSP to have implemented exactly what is needed for its operational risk environment. This tailoring of the system ensures that no capabilities are missed, and no activity is wasted on non-relevant aspects, thus maximising both technological and process operational efficiency.

But this methodology does not compromise on analytical capability, profiling, distinct rules and controls, reports and data queuing capability are included within the system to ensure accurate and effective decision making in a timely manner. As no pre-described process methodology is enforced on operational management, this also allows the operational process to be tailored to suit each operator's resource profile, thus again maximising efficiency, which is essential for smaller operators where resources are limited.

CONCLUSION

XINTEC is determined to enable the smaller operators worldwide to achieve the same level of risk avoidance and prevention as larger scale operators, by providing a risk management software suite tailored to the needs of their market space.

We believe that smaller operators should not have to compromise or tolerate inefficient or ineffective systems that do not meet their operational need, purpose or direction.

Therefore our purpose is to provide solutions that empower the smaller CSP's enabling them to improve and reduce their financial exposure to risks in the short and long term, without significant impact on resource or financial cost.

XINTEC Fraud solutions are the only true market place Fraud management Systems designed for smaller operators that deliver risk management operations with optimal efficiency in cost, resource and capability, allowing the operator to manage their risks effectively.

WWW.XINTEC.COM

IMPROVE PROFITS, REVENUES AND CASH FLOWS

XINTEC are world-class providers of cost-effective Fraud Management and Revenue Assurance solutions to the telecommunications industry.

We enable Tier 2 and emerging communications service providers to improve their financial performance by preventing and recovering revenue losses.

PREFERRED SUPPLIER

vodafone

XINTEC

+353 (0)1 293026 | WHELAN HOUSE | LEOPARDSTOWN