

Why risk and revenue assurance officers lie awake at night

Service providers have more need for integration between fraud detection and revenue assurance in today's world of Internet anonymity, social networking and growing crime rings.

Oct 13, 2010 5:05 PM,
By Susana Schwartz

With industry figures putting telecom fraud losses at \$72 billion USD ([CFCA](#)), it's no wonder service providers worldwide are concerned about both internal and external fraud. The numbers are probably greater, as most companies are reluctant to publicly report losses or threats—whether internal or external, and often, those in charge of fraud have to investigate the same people with whom they work and eat lunch.

With “thicker and bigger” wireless and wireline networks comprising more IP-based services (VoIP, VoB, etc), and increasing pressures to open up resources to partners for more innovative services, there inevitably are more exposed assets than ever before—particularly with the amount of sensitive data about customers now being collected and with disparate systems across different environments holding that information.

“There is more temptation, not only at the top, but at the lower levels when you have people sitting on so much information that others covet,” acknowledges Tal Eisner, senior director of product strategies for cVidya, [which today launched FraudView v9, its first major release since the acquisition of ECtel and the launch of its IRIS suite](#). “You can have internal folks leaking information about celebrities to reporters or giving discounts to family members and friends; you can have traditional fraudsters carrying out the usual fraud; or sophisticated rings of organized crime working across state and international boundaries. With new devices and the anonymity of the Internet, crime will continue to increase. Just look at how much iPhone subscription fraud has been covered or the reselling of other hot products, and it's easy to see why this is a growing area of interest.”

Fraud and risk managers work in environments transitioning to new services, so fraud schemes are much more complex and more organized than ever before, especially with the advent of social networking and more sophisticated links among individuals and organizations carrying out fraudulent activities.

According to Eisner, there will have to be more integration of revenue assurance and fraud assurance because of the natural synergies between the information gathered by revenue assurance managers and those in charge of fraud detection issues. “That integration is necessary because being reactive is no longer good enough; you have to have to be proactive and have the types of tools and analytics in place that help you accommodate new developments and the threats that come with those developments,” said Eisner.

The technology is evolving, as more sophisticated solutions now digest much more information than was ever possible before. There are benchmarks for how fast information and xDRs generated by SMS, MMS, emails, data, voice, money and data transactions can be collected and analyzed—not only in a granular manner, but now in a more holistic way so patterns and linkages can be seen. “Increasingly, there is the capability to monitor more and to do link analysis, where fraud schemes and organized crime can be detected not just among individuals carrying out ordinary theft, but more elaborate schemes that cross geographic boundaries and technologies,” said Eisner.

Also, by integrating more with social networks and search and location technologies, vendors are coming up with innovative solutions. In the case of cVidya, for example, investigators can integrate sophisticated algorithms and analytics with Google Maps to get location-based views on screen the place exactly where fraudsters are working and with whom they are linking up in terms of people, organizations and personnel for external or internal fraud.

As telcos increasingly partner with financial institutions, merchants and over-the-top content players, the risks and types of fraud will become broader, as each of their partners can pose a risk to their environments.

Any time there are compromised networks, there are links between resultant fraud and criminal activity and the telcos over whose networks it occurred, and on a customer level, there is an impact to the perception of customer experience when fraudulent activity causes a downgrade in services for both individuals and enterprise customers.

The growth of mobile services and proliferation of mobile commerce for mobile banking and things like telemedicine will only increase the risks.

To prevent loss of revenue and reputation, telcos increasingly have to work to stave off issues before they happen. They have to proactively analyze disparate data and identify patterns to prevent fraudulent activity by consumers, dealers and organized crime, and to support law enforcement in their pursuit of these criminals.