Why risk management and revenue assurance can't be left behind when upgrading your B/OSS

By: Bernardo Lucas

It is no secret that the communications industry is experiencing a transformation without precedent. And with recent reports like that by Juniper Research noting that revenue driven by 5G will reach $300 billion by 2025, communications service providers (CSPs) across the globe are collectively investing $50 billion in operations support systems/business support systems (OSS/BSS) by 2024 in order to support the next-generation services, partner ecosystems and business models that 5G will foster.

In the headlong rush to invest in OSS/BSS, however, it's critical to ensure that a comprehensive risk management solution that integrates fraud management and revenue assurance is part of the plan— and not left on the back burner.

As CSPs begin to utilize their 5G network investments by launching services such as IoT, CSP marketing teams will start to roll out new innovative billing models. The monetization opportunities brought on by 5G open the door to a fresh approach beyond the standard rating and charging designed for connectivity usage. For example, with 5G, opportunities arise with network slicing, quality of service (QoS), WiFi hotspots, and services provided through multiple service providers. We've already seen some examples of innovative business models around various content streaming packages, where different resolution, type and number of shared devices become part of a CSP's service bundle.

5G network slicing is an interesting use case that demonstrates the potential for new business models to be applied in the 5G era. For example, let's consider a surveillance camera service provided by a CSP that uses two different network slices, each with different performance and cost characteristics. In this case, an Enhanced Mobile Broadband (eMBB) network slice provides low-cost connectivity, suitable for always-on low-resolution access, and uses specific tariffs and units of measurement for charging. When it's necessary to zoom in on the camera image, users can rely on high-resolution access, which is provisioned in a more expensive Ultra Reliable Low Latency Communication (URLLC) network slice. This URLLC network slice is configured at a different charging tariff and uses a different unit of measurement for charging.

This particular use case is just one example among many possible scenarios where CSPs can allocate different 5G slices to different services at different billing models and prices. Ultimately, these new use cases will require defining which devices on a data plan are allowed higher data demands, tracking the levels of network congestion at any given time, and offering slower bandwidth options through a variety of competitive pricing models to meet customer demand. From a billing and charging perspective, these changes will put tremendous pressure on CSPs to upgrade their policy and charging solutions in order to keep up with the demand that connected devices will generate—and monitor and control any potential for revenue leakage with their customers and B2B partners.

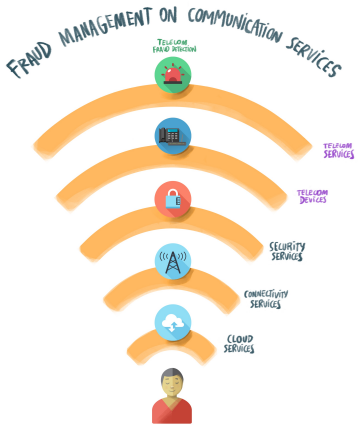
As a CSP's value proposition shifts towards an ecosystem-driven model that includes not only connectivity but also partner management, shared customers, and shared revenues, these opportunities will come with new risks from the many stakeholders, and also new requirements for risk management.

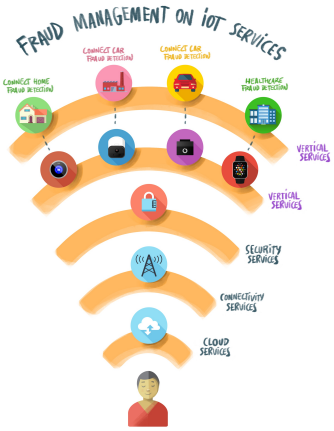
By releasing new services beyond the traditional communications portfolio, 5G adds the availability of real-time data streams and increases the number of customer interactions with CSPs. This potentially results in a better customer experience and contributes to increased retention, and also allows for a 360-degree view of the customer for risk management purposes, such as fraud. The analysis of the new data streams increases the understanding of risks and the customer base, which can lead to the assurance of the next generation of products and services.

However, CSPs need to be aware that, by releasing new services that fall outside of their traditional communications portfolio, the datapoints for risk management no longer remain solely in their own OSS/BSS. All communications data is now the sum of data generated by the relationships of the partners themselves. How they process the data they receive—and how they respond and act upon it—in itself will affect how far CSPs extend their risk-management coverage. Take, for example, identity management: unlike traditional mobile voice services, where the user identity is kept in-house with the CSP, with the IoT the role of identity management expands along the value chain. In short, it is no longer just about identifying people and managing their access to services. In the 5G world, identity management must be able to identify devices and sensors, monitor and then manage their access to sensitive and non-sensitive data along the overall value chain—which is becoming increasingly complex.

Using a traditional risk management governance model and strategy to assure 5G networks, services and business models will largely fail, because the key auditing functionalities have been relegated to isolated selections of tactical technologies, management features, and operational procedures along the value chain. Every day, the level of sophistication and organization among fraudsters increases. Gone are the days when a simple set of rules built on top of OSS/BSS data would be enough for CSPs to stop revenue leakages from telecom fraud. For many years, CSPs focused primarily on event monitoring within clear organizational boundaries and business support systems. This legacy approach must change, however, as CSPs move up the value chain and position themselves as IoT service providers in order to properly monetize 5G opportunities.

The infinite number of potential use cases for connecting things to the Internet and the growing ecosystem of players will bring added complexity that will increase the opportunity for bad actors to find new ways of cheating the system. For example, IoT and eSIMs welcome new opportunities for traditional types of telecom fraud—such as subscription fraud, international revenue share fraud (IRSF) and traffic pumping—to make a resurgence. Add to this the growing use of digital channels, and CSPs are left vulnerable to new types of online fraud such as synthetic identity fraud and account takeover. With 5G, it becomes more apparent than ever that CSPs will require robust risk mitigation methodologies and auditing capabilities for billing and rating validation. This is only possible with the power of advanced analytics and automation, which turn data into powerful risk management insights and actions in order to predict, detect and safeguard against vulnerabilities.





Source: WeDo Technologies

Not only are advanced analytics, AI, machine learning and automation required to process and manage the sheer volume, velocity and variety of data that a 5G network will generate, these capabilities will also improve CSPs' ability to spot known fraud threats—as well as prepare for new, unknown ones. It is also important to note that fraudsters already have AI and automation in their weapons arsenal, giving them the ability to organize their actions over a huge scale—and then essentially train a computer to keep repeating and optimizing the process as it searches for new opportunities to commit fraud. When one type of fraud, like subscription fraud, can lead to another more damaging kind of fraud, like IRSF, it becomes absolutely essential that operators have access to their own ML/AI tools as well.

All too often, IoT risk management concepts and strategies are discussed but not deployed. Don't lose the opportunity to truly capitalize on your 5G investment by failing to address risk management requirements today.