3 Strategies to Accelerate ROI From DT

By: Bernardo Lucas

As the communications industry's digital transformation takes shape, and the limelight shifts from connecting the users to connecting a user to their digital lifestyle, technology innovations such as eSIM, VoLTE, IoT, cloud, NFV, and 5G raise important business assurance questions for Communications Service Providers (CSPs). There are three top considerations for CSPs that want to accelerate the return on investment of their digital transformation.

#1: Focus on CX to drive revenues

Traditionally, the digital transformation of a CSP focused on process automation in the back office or core network. The launch of eSIM, however, promises to take it a notch higher for the end consumer: they no longer need a physical SIM card to get access to a network, or to switch service providers. A good experience is what the consumer desires; and not just for services on their smartphone but increasingly also on their digital watch, athletic wearables, connected car, digital house, and more. The customer expectation is that their "lifestyle" works everywhere—in their country as well as while roaming.

For a CSP, the digital transformation of its network involved embracing VoLTE, and LTE-A technology to provide their consumers high-definition voice, fast call setup, and higher data speeds. 5G is only going to enhance this experience with new services and experiences.

Gartner projects that in 2020, network operators will spend $4.2 billion on 5G wireless network infrastructure. However, 5G revenues are not expected to build real momentum until 2021. With this splash of cash by operators in the race to launch 5G services, monetizing the opportunity and achieving a fast return on investment is paramount. Instead of competing on network speed or devices, communications service providers need to now offer differentiated services by providing tiered service offerings and greater personalization to motivate subscribers to either pay a premium for 5G services or choose the CSP's 5G network over other competitors. Edge computing also facilitates this.

While some analysis will still need to happen at the core, IDC's FutureScape for IoT report believes that by 2022, 40 percent of initial IoT data analysis will occur at the edge. This is because as millions of devices at home, work and in the community are powered up, decisions will need to be made in fractions of a second as to where to send a device's traffic to maintain uptime, ensure it is safely connected, operate within and across network slices, and stay constrained by the business parameters such as shared data plans, etc. The user will no longer be looking for a separate *subscription* plan for each connection but will look for an *account* plan that encapsulates their digital lifestyle. Edge technology enables these hyper-personalized, interactive experiences where content providers can react and engage with customers securely and with sub-millisecond latency, creating a superior experience that's within the end user's control. This opens the door to creating more effective ways of reaching consumers, providing timely offers with higher acceptance rates and a better customer experience.

Roaming is another area where CSPs can improve the customer experience. According to Juniper Research, roaming data revenue is expected to increase to $31 billion by 2022, rising from $21 billion in 2017, mainly fueled by customers attracted to 'Roam-Like-At-Home' plans or Day Passes. The IoT is expected to account for an additional 20 to 30 percent of total roaming revenue as the digitally connected world takes shape. The IoT will put increasing pressure on the customer experience, particularly as mobile 'things' and applications go beyond traditional handsets, such as autonomous cars and wearables, and begin to cross borders.

Communications service providers can no longer just pass the baton to their roaming partners to manage their customers when they are abroad. Instead, CSPs need to employ the benefits of intelligent monitoring tools that capture data about a subscriber's quality of experiencewhen they are roaming, down to the individual IMSI and not just the network level. With this level of data, CSPs will have the insights to steer valued customers who experience poor quality service onto better networks, while more quickly identifying the root cause of issues. This helps reduce customer care costs, while also identifying and proactively compensating valued subscribers who had a poor roaming experience. At the same time, some services may require that all of a subscriber's devices roam on the same network, and in such cases, the CSP needs to ensure that they select the best roaming network for each individual subscriber and are able to steer *all* devices for *that subscriber* onto the same network.

#2: Avoid leaving money on the table (especially as business models change)

5G will be a game changer when it comes to the traditional partner ecosystem and the business models that support it. For example, greater collaboration between CSPs and third-party content providers will become commonplace. With these arrangements, however, come a multitude of opportunities for revenue leakage to occur as the digital ecosystem expands beyond traditional telecom providers and the one-size-fits-all service business model is shattered.

Let's take a 'Super Bowl of the future' as an example for how CSPs could be at risk of costly revenue leaks. In this scenario, let's suppose a content provider has offered three levels of tickets to live stream the event: standard, premium and gold. Standard tickets provide live streaming access to all of the on-field action; premium tickets provide access to the team's huddle; and gold provides 4K video and Virtual Reality experiences. Next, we assume each tier of service runs on its own network slice and has its own quality of service SLAs and pricing configurations: one for subscribers and one for content partners.

As you can see, network slices will be an important mechanism to support the catalog of new enterprise and consumer applications. However, with all this flexibility comes added complexity. Beyond the basics of provisioning services and managing any upgrades in real-time, CSPs must also measure and rate the content being distributed at each ticket grade to ensure accurate billing and margin analytics. When we add

network slices to the mix, where different service level agreements will apply to different slices and different pricing models will depend on specific slice requirements, revenue assurance in the age of 5G has become that much more complex.

In order to ensure SLAs are being met, CSPs require the ability to collect performance data from 5G networks and network functions in real-time. It is not just the home CSP, however, that requires access to this information. In the case of international roaming, the same or similar features of the 5G slice supporting a roaming car should also be available in the visited operator's domain. Continuity of service when moving between different communication service providers (i.e. international roaming) is an important feature that needs to be provided and assured within the properties of each 5G slice.

Many services are based on the expectation of universal access to network services without the need for complex business arrangements between communication service providers. With 5G, however, this is increasingly looking impossible. When a breakdown occurs on the Service Level Agreements (SLAs) between the CSP and partners, CSPs not only bear the brunt of the customer's dissatisfaction but also can lose mindshare with their partners and run the risk of penalties and partner churn. The complexity of managing network slices and accurately charging, billing, and settling for the services underscores the importance that CSPs need to have 5G-ready revenue assurance strategies in place so that any revenues generated are captured and not lost to leakage. This becomes more complex when it comes to cost, margin, and finally experience assurance!

#3: Don't leave the back gate open to fraud and security threats

IoT is undoubtably a rising security and fraud threat that CSPs must address immediately. Research published in January 2020 concluded that a security threat of smart light bulbs that was identified back in 2016 still lingers today. Where a smart light bulb may be an innocuous device to some, it can provide a lucrative entry point for hackers to commandeer entire networks. The security and fraud risks don't stop there. Hackers today are still abusing vulnerabilities in SS7 and Diameter protocols to send SPAM, spoof calls, track subscribers' locations, intercept SMS and calls, and conduct subscriber fraud, routing attacks and denial of service attacks.

A network is only as secure as its weakest roaming and interconnection partner. While 5G security protocols offer controls far surpassing those of previous generations, network operators will still be exposed to SS7 and Diameter vulnerabilities till the 5G networks become ubiquitous. Consequently, CSPs have to consider security with a broader view that looks at cross-protocol threats, threats to network as well as to its subscribers, and threats to its partner eco-system. The 5G SEPPs have to secure macro as well as micro network boundaries, and the trust zones have to be established at the slice level, and not just the N32 network boundaries.

When it comes to network slices, in an era where multiple MVNOs will share infrastructure, strict isolation at multiple levels will be required to ensure absolute security and privacy. This is where fraud and security management must be closely integrated and prioritized in the age of 5G. As technology gives the mobile handset an increasingly pivotal role in banking, payments, identity management and two-factor authentication, promoting trust in the handset and in the network now becomes mission critical for CSPs, especially as IoT takes flight. Consumers are no longer tolerant about security breaches. They expect the same security safeguards when it comes to their smart light bulbs as they would during remote surgery. In fact, according to recent research sponsored by Mobileum, 58 percent of enterprises and 52 percent of consumers said that they would leave their operator in the event of a security breach.

To address the risks, fraud and security teams need to compete with the level of sophistication of the tools that today's hackers are already utilizing. AI, machine learning, automation and cross-protocol firewalls are just a few instruments that will be key to monitoring, detecting and minimizing the risks of security and fraud attacks in the 5G era. When supercharged with AI, machine learning and automation, fraud

teams will have the ability to detect threats, uncover unknown, emerging threats and take action to shut them down faster. With cross-protocol signaling firewalls, CSPs have the added protections to monitor and control SS7, Diameter, Voice (SIP/ISUP), IMS, GTP, and 5G HTTP signaling streams in order to guard subscribers and services from these threats.

Industry analysts project that the short-term outlook for 5G will consist of high CAPEX investments followed by flat 5G revenues. In order to accelerate their 5G return on investment, Communications Service Providers must invest in the technologies and tools that help them to monetize 5G premium experiences, assure their revenue gains and protect themselves—and their customers—from the growing list of fraud and security threats.