www.pipelinepub.com
Volume 17, Issue 6

3 Ways to Derisk the Digital Economy

By: Rui Paiva

Recent GSMA figures found that communications service provider (CSPs) revenue outside of core services hovers around the 20 percent mark. To drive ROI on the $1 trillion in investments in 5G, CSPs are eyeing B2B revenue opportunities in the manufacturing, financial services, retail, healthcare, oil and gas, agriculture and mining sectors to target their big push into digital services. However, supporting applications in these verticals comes with risks that neither CSPs nor the enterprise customer can afford to let slip through the gaps.

The transformation opportunity

5G presents an opportunity for CSPs to capture new revenue streams from industrial digitization. In cases such as network-as-a-service (NaaS), network exposure is becoming a reality through the transformation of core telecom network assets into digital assets. With 5G, the dynamic provisioning and scaling of network capacity and resources are available for the first time. The vision of managing the NaaS in the same way as a developer might manage cloud resources on Azure, AWS, or Google Cloud is happening through a combination of scalable infrastructure and the next generation of digital business support systems (BSS).

The 5G network evolution has presented an abundance of new business opportunities for CSPs in verticals such as industrial automation, security, healthcare, and automotive. To capture the opportunities and leverage their NaaS capabilities, CSPs are deploying automated BSS support systems capable of expanding non-telecom value chains, while supporting new business models through open interfaces.

The world's digital connections are becoming broader and faster, providing a platform for every industry to boost productivity and innovation. To illustrate the range of possibilities, let's look at the healthcare industry, where connectivity-enabled innovations can make it possible to monitor

patients remotely, use AI-powered tools for more accurate diagnoses, and automate many tasks so that caregivers can spend more time with patients.

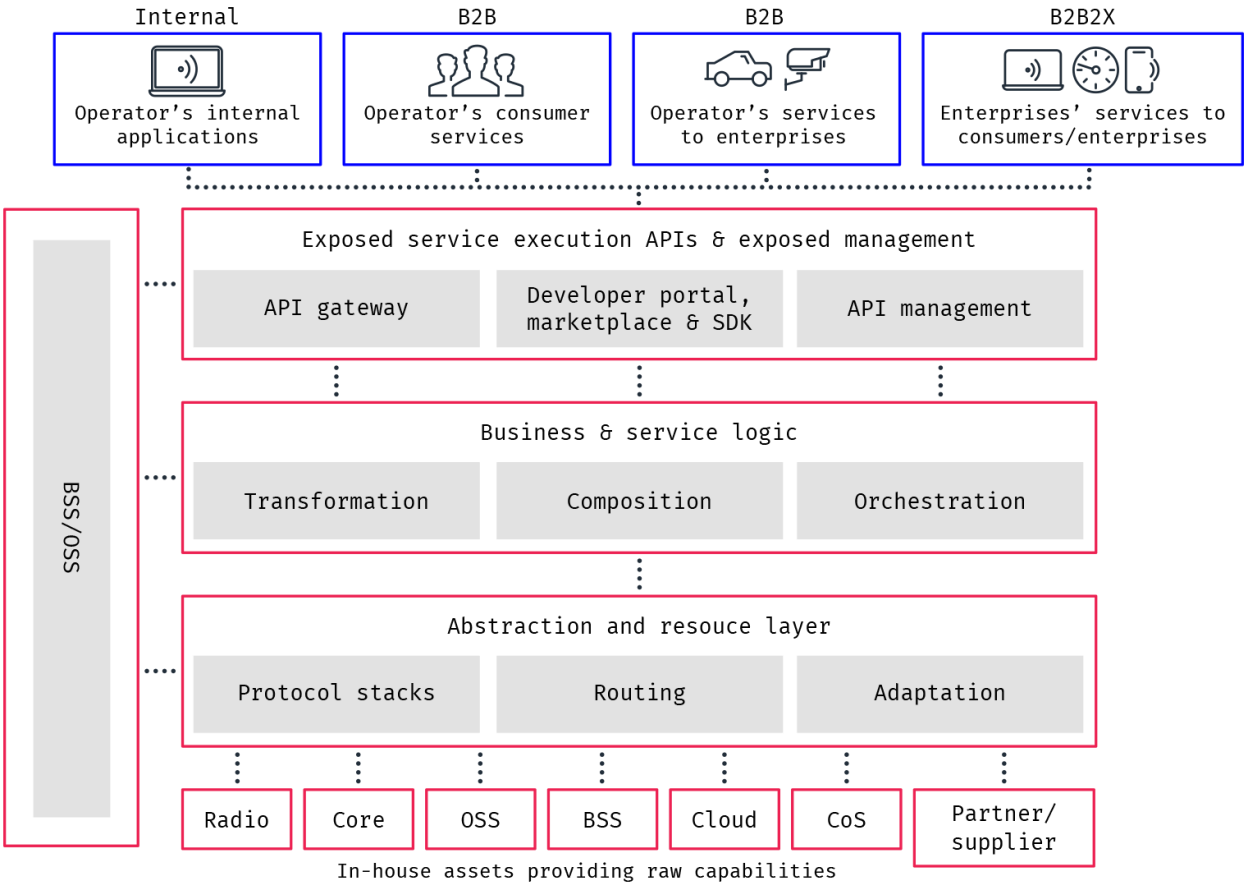

Figure 1: New business opportunities

click to enlarge

This technological transformation of the healthcare sector offers numerous opportunities for telecom operators to penetrate new value chains and initiate partnerships that benefit the entire ecosystem. Still, it is just one example of how CSPs can partner with a wide range of vertical industries.

In light of these emerging opportunities, CSPs must mitigate important risk factors to ensure that the risks do not outweigh the reward of digital transformation.

De-risk Strategy #1: Eliminate risky grey areas of accountability

Expanding the business models through partners can bring CSPs significant benefits and help bring about exciting innovation, but inevitably offers less direct control than delivering it in their own controlled environment. It is often said that a business is only as strong as the chain of suppliers it works with.

An example of how service delivery chains are becoming complex, and by doing so, becoming more difficult for handling risks, can be exemplified by Uganda's recent hacker attack on the country's mobile money business that processes phone-based transactions. The mobile money value chain is made up of mobile network operators (MNOs), banks, and end users and is a technology that allows people to receive, store, and spend money using a mobile phone.

In the mobile money value chain, there are blurred risks mainly due to the ambiguous roles of banks and telecommunications companies in financial services, as proven by the recent hack of a gateway that links the bank-to-mobile money transactions. There is a clear line between "banking" and "mobile money" as a standalone business. Where lines become blurred is when MNOs expand their services to connect with banks and allow the withdrawal of money from regular ATMs.

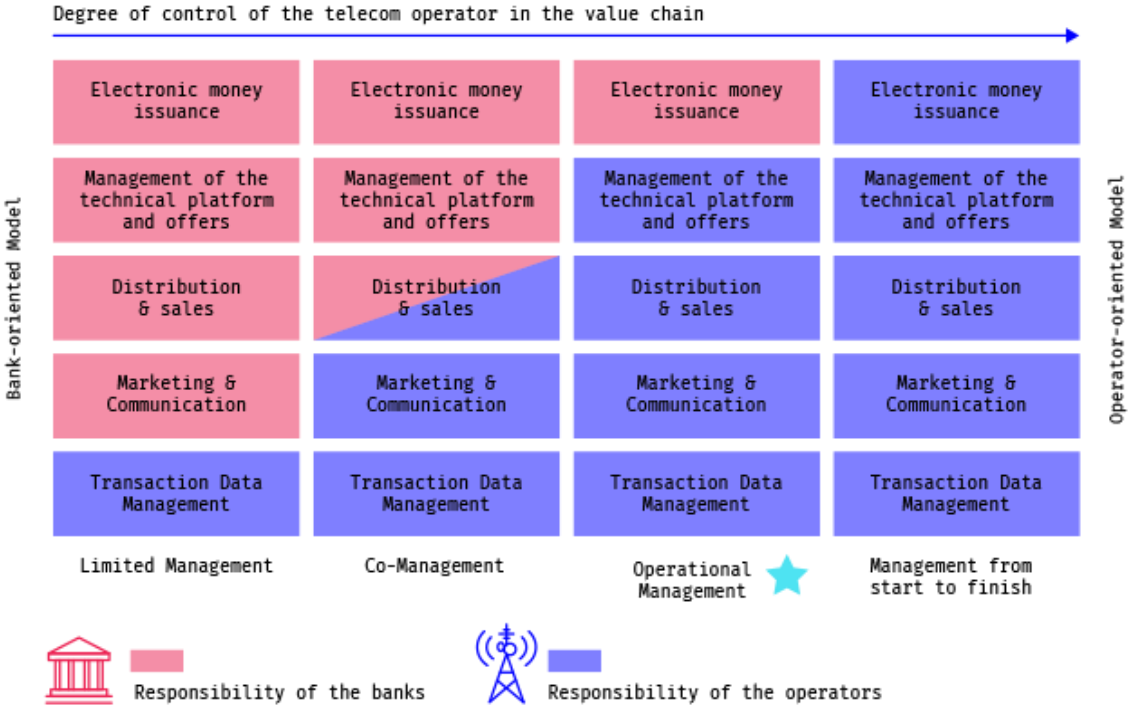

Figure 2: Mobile money value chain

click to enlarge

De-risk Strategy #2: Proactive dynamic decision-making

With digital transformation, telecom risk management initiatives are going through a massive generational shift. Traditionally, telecom value chain risk management has been heavily supported by analyzing internal events, such as network and OSS/BSS, and optimization models on internally processed data. The shift between just relying on telecom partners and having many vertical partners is pushing in favor of a more vertically integrated technology stack: the cloud. This transition offers all the stakeholders better security and innovation at a lower cost, allowing them to act fast on potential risks.

Not only will 5G-driven digital transformation deliver a massive increase in the volume of transactions, it will also generate a massive diversity of exchangeable events from a variety of partners and services that need to be monitored and analyzed in real-time.

For example, new services that rely on non-face-to-face customer relationships require securing digital identities based on the information exchanged between a CSP and their partners. This way, a CSP can ensure the unique and consistent identification of a subscriber, authentication, and policy assignment based on the identities, whether we are talking about a user or a thing.

The opportunity to leverage the digital transformation data exchange creates the capacity to analyze distributed big data for integrated risk management (IRM) purposes, rather than pursuing a more reactive approach that focuses on finding more data sets and understanding how to use them to address risk. An IRM strategy reduces siloed risk domains and supports dynamic business decision-making via risk-data correlations and shared risk processes.

Along with the connectivity platform, CSPs are in a prime position to understand and manage a wide scope of risk through a comprehensive view across business units, risk and compliance functions and key business partners, suppliers, and outsourced entities.

The goal should not be to create one big repository that can handle any data set, no matter how large. Instead, it should be to fully automate the linkage among relevant insights from a wide variety of internal and external sources and process that data in various nodes of the supply chain. Doing so triggers action immediately when possible and adds data to a queue for deeper analysis.

De-risk Strategy #3: Break data silos

To better address the needs of their stakeholders and organizations, CSPs must evolve their risk management programs to more integrated approaches. By doing so, CSPs will have better control and visibility, the ability to monitor risk-based decisions based on their digital business initiatives and partnerships and gain further alignment with business outcomes when making risk mitigation investments.

Traditional governance, risk, and compliance (GRC) projects have largely been developed on siloed approaches, missing the capability to link the business auditing practice with the continuous control of the value-chain risks.

Moreover, these GRC processes are often supported by investments in disparate sets of tools focused on specific capabilities, such as data collection or visualization. Still, they do not bring the business logic seen today on vertical CRM or ERP solutions. As CSPs are starting their journey toward 5G, they need to intelligently connect the data points into an integrated set of insights that link the expanding portfolio of assets, processes, and performance objectives that drive their business operations.

5G will deliver CSPs the capability to leverage new services as well as granular network control to generate multiparty B2B2X service revenues. At the same time, 5G will drive new risks from a combination of fragmented value chains and partners. New technologies like 5G may provide

powerful benefits to enterprises, but they also influence workflow and processes, resulting in risk. Threat modeling is an essential exercise supporting a thorough risk assessment process that should benefit organizations.

Resilient organizations anticipate risks, develop controls, monitor events, and, whenever possible, apply automatic actions to remediate risks. Today, intelligent risk management value is derived from the intelligence analysis of the different elements of market value-chains powered by data analysis. The data generated by several application silos are combined and greatly enhanced to understand risk better. Building an automated capability requires more than a flair for writing algorithms. It requires an array of technical (quantitative, IT, and business) and nontechnical (communication, leadership, and teamwork) skills manifested in a mix of data science and other supporting roles. The right blend of technology and business skills is essential to choose the right partner to bring quick and positive business impacts during the deployment of a digital ecosystem risk management strategy.