Operators should match their IoT security strategies with their ambitions in the IoT market

October 2017

Sherrie Huang and Michele Mackenzie

We forecast that 6.4 billion IoT connections worldwide will use fixed, mobile and low-power wide-area (LPWA) networks by 2025.[1] As the IoT market grows, so does the security risk. The discussions on how to secure the IoT are increasingly the focus of attention. An end-to-end IoT project consists of multiple, often diverse, devices, various platforms, layers, and interfaces, creating many dimensions to secure. Security has moved up the list of priorities for IoT projects. Telecoms operators, as IoT service providers, need to develop their IoT security capabilities with relevant products and skills to match their IoT strategy and ambition.[2]

Telecoms operators need to develop security offerings to match their IoT proposition

Operators have a strong legacy in securing the connectivity layer with carrier-grade, embedded security solutions. Security requirements such as secure transmission, safe data and user authentication have been fused into the operator networks for decades and cellular networks are generally viewed as secure and reliable.

However, in the IoT market, operators increasingly address components beyond connectivity to capture a larger share of revenue. Moving up the value chain requires more specialist security expertise, which CSPs do not always have. Operators will increasingly need to do the following.

- Map their security offerings closely to the IoT components of the value chain that they provide, such as the application, device and enabling capabilities like hosting. Providing enhanced security for devices beyond SIM authentication may not be familiar territory.
- Tailor the security offering for their target verticals. This will require an understanding of the technical component of the offering but also regulatory compliance and business models. Those operating in the EU will need to understand GDPR compliance, for example.

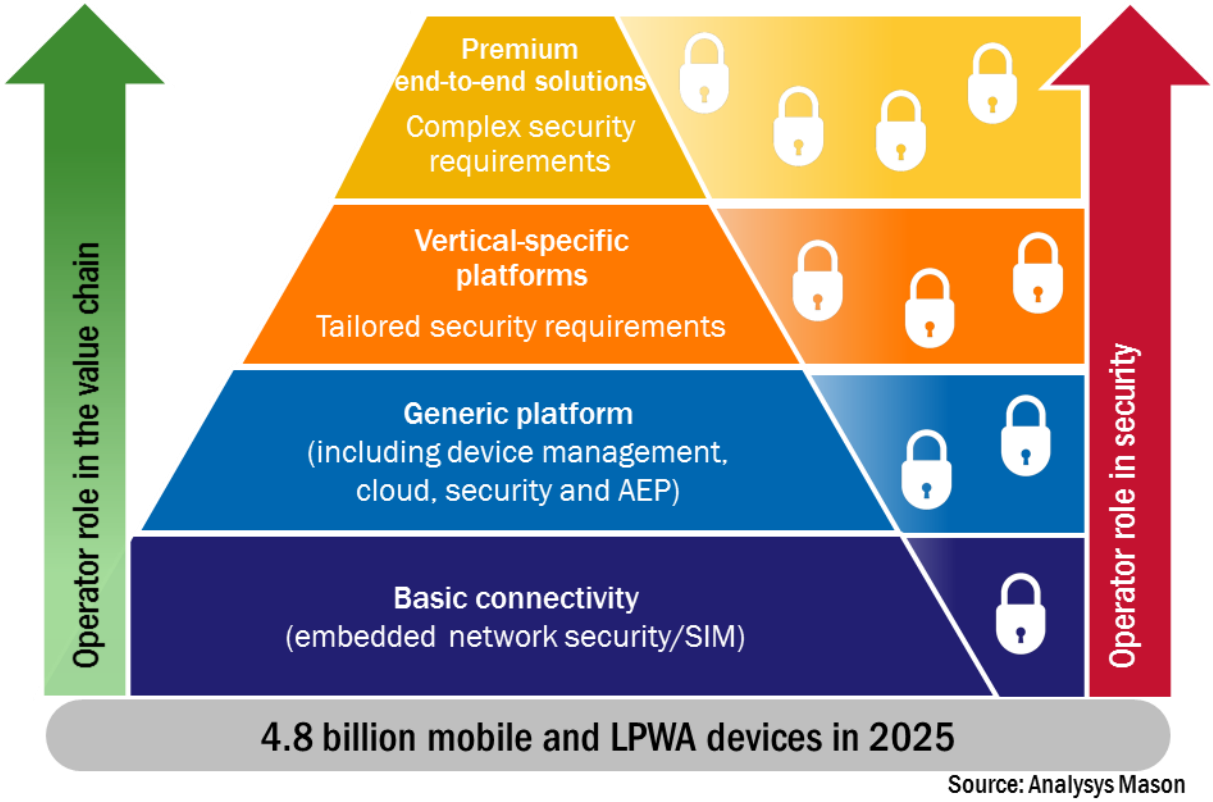
Operators will need to partner or invest to align their security offering with their IoT proposition. Operators that already benefit from an internal cybersecurity unit, like Telefónica and Vodafone, may have the necessary skills to build their own solutions but most will still need to partner for some or all solutions. A few operators, primarily those that have invested heavily in specific sector expertise, may make strategic investments or acquisitions to bolster their offering. Bold moves such as this will send a clear message to the market about their intentions and role in the value chain. Interestingly, this bold approach is not confined to the large global operators such as Telefónica or Singtel. Smaller national and regional-focused operators with strong IoT business units, such as KPN and Tele2, have acquired to strengthen their security credentials.

1 Analysys Mason's IoT forecast is available in our DataHub. Available at www.analysysmason.com/datahub.

2 For more information, see Analysys Mason's IoT security: opportunities for communications service providers. Available at www.analysysmason.com/iot-opportunities-csps-rdme0.

Despite the significant effort and investment required, it is unlikely that security will generate a significant new revenue stream in its own right. However, it will be critical in winning new business and potentially differentiating the operator's service from that of competitors.

Figure 1: The operator's role in IoT security must match the operator's role in the IoT value chain



Source: Analysys Mason

Security can help operators differentiate and strengthen their LPWA service

By 2025, more than half of the total wide-area IoT connections globally will be on LPWA networks.[3] This will bring new and different challenges. Many of the devices connected to an LPWA network will be low-power devices with limited computing power, factors that will restrict security options.

Operators using 3GPP standards (NB-IoT and LTE-M) have a clear opportunity in the early phase of LPWA market development to differentiate their offering from the proprietary networks by marketing the inherent secure nature of their networks. Operators have been slow to promote the value of embedded standardised security in their cellular networks (although the real value of security may have only recently come to the fore). Providing additional security layers by design from the outset of the project will likely add some additional upfront costs but will reduce the overall costs of delivering security for the lifecycle of the project. For example, building in extra layers to secure and update the connected devices.

Operators could position security as a core differentiator to their LPWA proposition and:

3 For more information, see Analysys Mason's DataHub. Available at www.analysysmason.com/services/Research/DataHub.

- **promote** the embedded security attributes of the network and the SIM and **market** the capabilities of their connectivity and device management platforms in detecting anomalies and mitigating the consequences – for example quarantining devices, OTA updates etc.
- **develop** new capabilities internally or through partnerships to provide additional, value-added security layers that are cost effective for LPWA solutions – for example, some operators are exploring the idea of offering additional security in the SIM
- **ensure** that their security offering addresses each component of the value chain where they provide solutions and **leverage** professional services and cybersecurity business units to advise on and implement security solutions.

IoT security could be an important differentiator

Selling IoT security solutions will not necessarily generate substantial revenue for operators. Security at the connectivity layer is embedded but should be a feature that could bolster the value of the connectivity offering. Security for other components of the value chain will be a premium service but is unlikely to generate significant revenue. However, IoT security will be a critical factor in winning IoT business with the potential to differentiate the operator's service from its competitors.