Security matters

As mobile operators expand their networks and launch new consumer services, experts say they need to adopt more integrated approaches for enhanced security.

With criminals targeting mobile networks, widespread use of SIMboxes, and increasing global cyber crime, the issue of security remains a major concern for operators. DAVE HOWELL reports

As smartphone ownership expands across Africa, the issue of security continues to be a priority for MNOs throughout the continent. While the Communications Fraud Control Association (CFCA) estimates global telecom fraud losses of USD38.1bn in 2015 or approximately 1.69 per cent of revenues, cyber security in general continues to have a high profile as the digital economy and its users come under attack.

According to Trustwave's latest *Global Security* report published earlier this year, the majority of compromises in regions outside North America were in online sales. "E-commerce environments were compromised in 70 per cent of cases in Europe, the Middle East and Africa, with 35 per cent of mobile applications tested having critical security vulnerabilities," said the provider of cyber security solutions which was acquired by Singtel last year.

It will come as no surprise that greater mobile connectivity and broadband access will lead to more cyber crime. For instance, the Kenya *Cyber Security Report 2015* said telcos are a "prime target" for cyber criminals as the country's reliance on technology continues to grow, and all organisations, such as banks and government, depending on internet connectivity from telcos.

The report stated: "Cyber criminals are targeting these organisations because of three main reasons: they control and operate critical infrastructure; they store large amounts of sensitive customer information, and they facilitate mobile money services in the country."

However, while Africa's MNOs are clearly aware of the threats to their networks and the services that they offer, the level of deployment of security systems in both the private and the public sectors to combat cyber crime is low.

Singapore-based Cataleya specialises in IP networking technology including systems for analysis, visibility and intelligence. It believes that given Africa's explosive growth in mobile penetration over the past few years, the main telecom expense management system vendors are now able to offer the same level of security platforms in the region as they do in other continents.

Miguel Lopes, Cataleya's VP of product line management, says: "Before, security systems were expensive and cumbersome to deploy. But nowadays in the age of NFV/SDN, these technologies are available at reasonable prices, offer flexible deployment models, and are now mostly part of the network by default."

But he goes on by saying that when it comes to fraud, the continent's mobile growth comes with a price: "No operator is an island. African MNOs must quickly adapt to protect their own subscribers from domestic, continental and global fraud attacks. The learning curve generated during this adaptation is the threshold from where fraudsters can act undetected."

Security management

The rapid expansion of mobile services into a consumer environment that has not had the benefit of developing robust security protocols has meant that Africa has become the new focus for cyber crime. One of the most common security breaches is SIMbox fraud *(see 'Killing your billing' right)*. This isn't surprising as the continent now has close to a billion subscribers, making it a very attractive target for this kind of network fraud.

The cellcos are fighting back. For example, after being hired by Ghana's government to track the use of SIMbox fraud, Accra-based consultancy Afriwave Telecom revealed it had seized 300,000 SIMboxes which would have reportedly cost the country's operators more than USD100m in lost revenues. And in a bid to tighten how SIMs are obtained, in March 2016 MTN announced it would only process cards during working hours. In May 2016, the company will begin to further tighten SIM card security by requesting an additional phone number and an email address to verify identity before a module swap is authorised.

While the main types of mobile fraud in Africa are likely to revolve around illegal SIMboxes and terminations, Lopes warns that domestic fraudsters are becoming increasingly sophisticated, and the arrival of international fraudsters also now presents a major threat. "New types of fraud such as the 'Wangiri' attacks, false answer supervision and others *[see 'Killing your billing' below]*, are occurring quite undetected. Africa's MNO's growth is attracting global fraudsters attention to a new market."

The vast market that the continent represents is of course commercially attractive for cellcos, and they also continue to innovate in order to provide competitive services to retain and gain subscribers. This has come at a cost, as such services are developing faster than the comprehensive security platforms that are needed to prevent fraud and cyber crime.

However as Andy Gent, founder and CEO of Revector, points out, most threats are the same worldwide and it really comes down to local dynamics such as the termination rates. "Where these are high we see more SIMbox fraud. So for example in the US (where international interconnect is rare), SIMbox fraud is virtually non-existent – the opportunity is simply not there. This is also true within EU countries. But in Southern Africa, where there are many countries, the opportunities for termination bypass are much higher."

Fighting the fraudsters

With a range of security threats across the mobile space, mobile operators have had to be equally innovative when combating fraudsters.

Approaches vary and include post analysis of CDR data. These report-based systems detect anomalies across a network, looking for unusual patterns that could be fraud. They are however, only effective after the fraud has taken place.

What is really needed are systems that can learn an MNO's systems and use machine learning and even AI to identify potential instances of fraud. As MTN points out, networks will be subjected to continuous vulnerability assessments as threats will continue to evolve. Hitesh Morar, the group's executive of IT and innovation, says operators will have to continue to ensure robust processes are in place to continuously identify, prevent, detect, respond and recover from threats.

"The advent of new technologies and the shift to all IP networks and services, as well as the shift to cloud services, brings with it a new dimension in security requirements that were previously only prevalent in the internet world.

Miguel Lopes, VP product line management, Cataleya

"No operator is an island. African MNOs must quickly adapt to protect their own subscribers from domestic, continental and global fraud attacks."

"The rise of digital services, such as m-banking, m-commerce and online service, requires security that extends beyond just prevention of DDoS attacks and encryption, and also addresses message authentication, filtering and digital signing."

Understanding the kind of mobile fraud that is being perpetrated is only one element of a solution. As Jacqueline Fick, chair of the GSMA Africa fraud forum explains, a change in attitude is also needed: "Cyber crime activity has become more focused on mobile platforms. But we have noted that our mobile security mindset is still that of using a phone and not a sophisticated device that contains valuable information similar to that stored on our computers;

KILLING YOUR BILLING

In its 'Fighting Voice Fraud with Big Data Analytics' white paper, Cataleya identified the following common types of fraud for MNOs.

False answer supervision
Early answer is caused by one of the interconnect parties sending a false answer signal. This causes all the previous switches to start billing even when the called party has not answered the call.

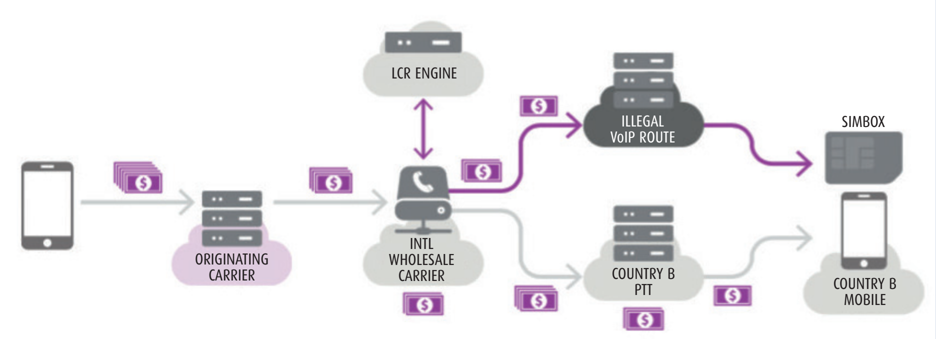
Wangiri fraud
Also known as 'robot dialling + callback'. The objective of the fraudster is to call thousands of users and hang up after one ring. Unsuspecting mobile users will return the call paying a premium rate per minute to a number which will be heavily disguised as a local one.

International revenue share
Fraudsters take advantage of certain premium rate country terminations such as Somalia or Sudan, for example, and inflate traffic into these countries. The fraudsters can play a role in the origination side by gaining access to a fraudulent SIM or hijacking a PBX system, or on the termination side by colluding with content or IVR providers in the countries with premium termination rates.

PBX hacking
Cases are generic and involve the bypass of a legitimate carrier in the delivery path of the call. SIMbox fraud *(see below)* is a of a typical case here.

Another case is location routing number (LRN) fraud. This is where the fraudulent operator sneaks in a LRN via a low-cost route and then sends it to the wholesale provider where it tries to terminate the call to the indicated network. But the call does not go through, and a 're-dip' has to be done to the LNP server which provides the correct termination network on the highcost route. The wholesale operator ends up bearing all the termination costs.

Subscriber identity theft (SIMbox fraud)
This is particularly rampant in countries with high numbers of incoming international traffic where SIM availability is loosely controlled and law enforcement is lacking. The fraudsters mainly use pre-paid SIMs where the ownership and address is hard to detect. There are many variations of SIMbox fraud and methods of detecting them therefore also vary.



a device that has to be secured in the same way as we have now learned to do with our computers.”

A change of mindset is only one component of developing a comprehensive approach to security. Carlos Marques, head of product marketing for business assurance specialist WeDo Technologies, also points to regulation: “Regulatory bodies can prove valuable in protecting against fraud, taking on a range of responsibilities including regulating prices, fighting against fraud and the fair distribution of telecoms revenue to different parties. However, due to the continual evolution of the industry, regulators need to be resourceful and forward-thinking to ensure they’re able to successfully execute on their duties.”

What is clear is that as the threats to mobile networks expand and increase in complexity, operators will have to move away from a general piecemeal approach to combating cyber crime in all its forms, to more integrated and intelligent systems. Here, cloud-based services are coming online from vendors that can offer an additional layer of protection to mobile networks.

Evolving threats

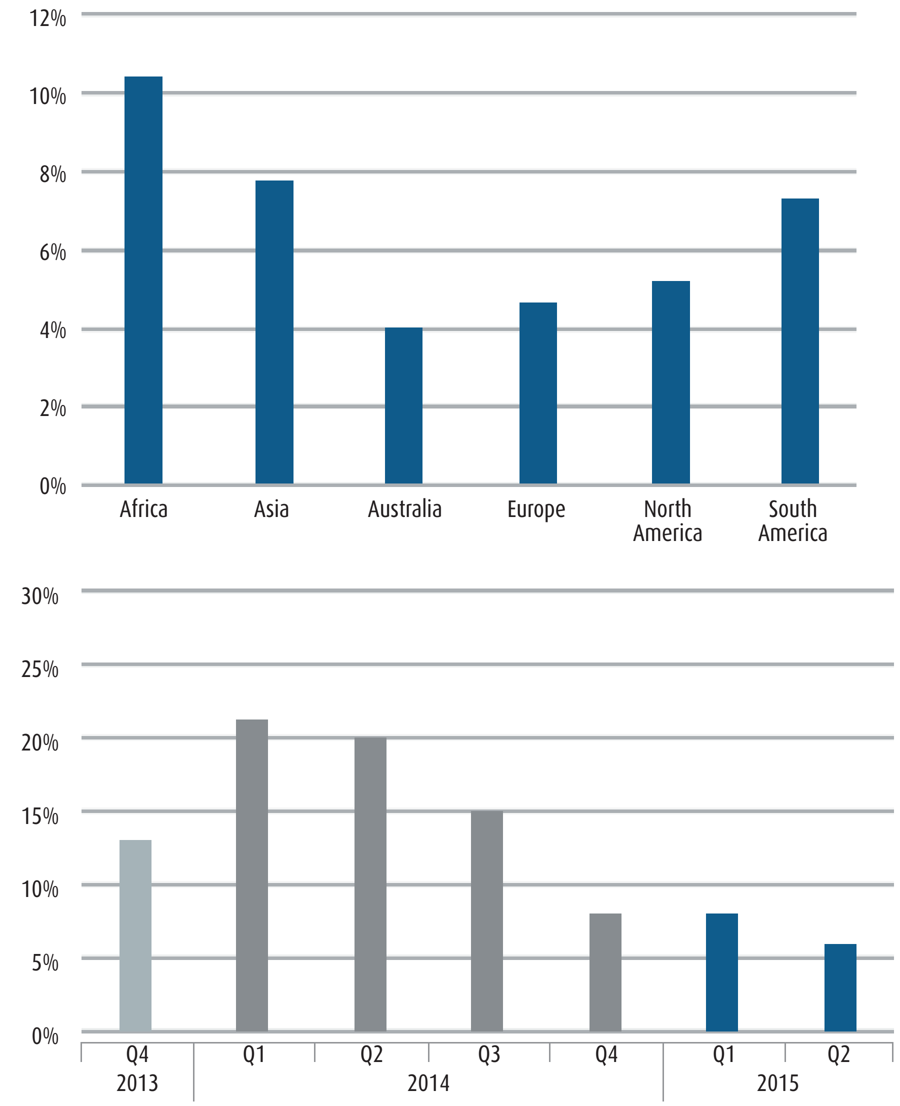
Clearly, the future will mean more security. But this must not be at the cost of eroding the services being delivered to consumers, as Simeon Coney, chief strategy officer with network security platform provider AdaptiveMobile, warns. “Carriers today are faced with the challenge of protecting the integrity of their networks, securing A2P messaging revenues, whilst future-proofing their investment in the next-generation of security architectures as NFV becomes a reality.

“Furthermore, there is an opportunity for carriers to play an important role in securing networks as we move closer to a hyper-connected future that requires new security architectures to protect 5G, IoT and beyond.”

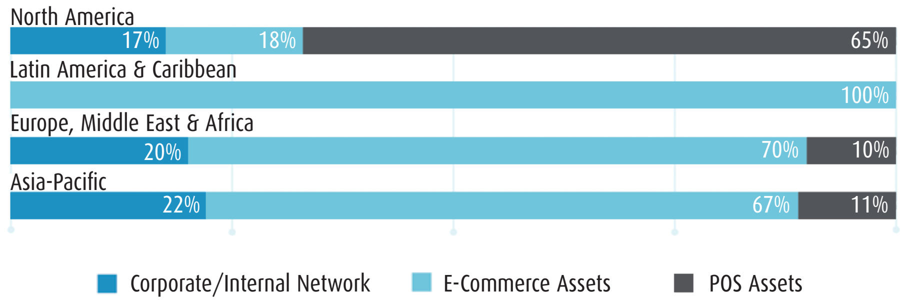
2015 saw near-exponential growth in all areas related to cyber security. In fact, Kaspersky Lab has seen a strong growth in detected threats in African countries. Dirk Kollberg, senior security researcher in the company’s global research and analysis team, says: “The continued increase in threats and cyber security matters certainly shows that African countries are a growing target for cyber crime and, as a result, countries like Nigeria need to pay attention to this reality and the future trends and predictions in this space.”

The massive growth of the mobile industry across the continent with new products developing means a multi-tiered approach to security is needed. New services mean new security threats as cyber criminals jump onto the next popular product to exploit.

“Africa is largely a pre-paid market and highly competitive on retail rates thereby challenging fraud resources to be on the constant lookout for arbitrage opportunities,” says the GSMA’s Fick. “LTE rollouts are accelerating, bringing increased demand for data and a host of new vulnerabilities associated with data environments.”



Top: Mobile malware infection rates declined about one per cent per region during the second quarter of 2015, with the exception of Africa which was unchanged and North America which dropped almost four per cent. **Above:** Global mobile malware infection rates. SOURCE: MCAFEE



Distribution of forensics investigations by region and type of environment compromised. SOURCE: TRUSTWAVE

She adds that SIMbox and termination fraud will remain a concern in countries where the cost of terminating an international call is considerably higher than that of a national one.

So the challenge that Africa’s MNOs face is two fold: they need to continue their programmes of network development as demanded by their subscribers, and roll out these services with robust security; but at the moment the security foundation that many of these services are built upon isn’t as strong as it could be. The answer is likely to come from an integrated approach that includes new legislation, strong security protocols that can effectively combat cyber crime pre-emptively, and a change in attitude that places network security at the top of the mobile operator’s agenda. ■