Risk Management in 4G LTE

Fourth-generation Long Term Evolution (4G LTE) is an open architecture, all Internet Protocol (IP), broadband wireless data technology designed to offer users access to technology-agnostic seamless roaming across carriers and geographic regions. The recent proliferation of promising wireless technologies has quickly been followed by torrents of new mobile malware and cyberthreats. 4G LTE is expected to exceed US $340 billion in service revenues by 2017.1 According to the Global mobile Suppliers Association (GSA), 415 mobile network operators (MNOs) are rushing for a slice of revenues, with 248 commercial deployments in 87 countries by the end of 2013.2 The business benefits of 4G LTE (see figure 1) are attractive to a global base of MNOs and subscribers.

To this point in time, mobile devices have been primarily used for voice traffic and have seen relatively low volumes of cyberattacks. However, with growth in mobile data traffic on LTE and increased computing power on smart devices, mobile technologies are becoming concerted targets for cyberattacks. McAfee reported a 4,000 percent increase in mobile malware in 2012 (over 2011) with up to 37,000 variants.3 The Cisco Visual Networking Index (VNI) forecasts monthly global mobile data traffic to surpass 10 exabytes in 2017 with 4G carrying 45 percent.4 With the number of entrants, size and market momentum building around 4G LTE, data on this platform need rigorous protection.

Risk management encompasses managing not only external attacks, but also inherent security risk and vulnerabilities resulting from network architecture, operations and service deployment.

While the 3rd Generation Partnership Project (3GPP) incorporates security into the LTE System Architecture Evolution (SAE), it also prescribes options for addressing various security vulnerabilities by means of network deployment and operations that are discretionary to MNOs. This creates inconsistencies among the hundreds of MNOs in the security implementation in 4G LTE services and introduces various risk.

Further variations in business objectives, business models, network deployment, operations and regional legislation introduce risk that needs to be evaluated and appropriately managed (figure 2).

Figure 1—Value of 4G LTE Technology

<table>
<thead>
<tr>
<th>Lower Capex and Opex for MNOs:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Flat architecture with fewer network nodes</td>
</tr>
<tr>
<td>• Spectral efficiency</td>
</tr>
<tr>
<td>• All IP based with IPv6 support</td>
</tr>
<tr>
<td>• No need to maintain circuit-switched network</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Better Service Experience for Subscribers:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• High bandwidths of 300 Mbps peak downlink and 75 Mbps peak uplink</td>
</tr>
<tr>
<td>• Low latency</td>
</tr>
<tr>
<td>• Interworking support with existing 2G, 3G and non-3GPP technologies</td>
</tr>
<tr>
<td>• IP multimedia subsystem (IMS) offering voice, data, video convergence, content and applications, e.g., VoLTE, telepresence, gaming</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 3GPP standard TS 33.401 defining the security architecture and prescribing deployment options</td>
</tr>
</tbody>
</table>


Risk management is the ultimate objective of all information security activities and this is no different with 4G LTE services.
BUSINESS OBJECTIVES AND STRATEGIES

Products and services in the marketplace are sustained only when they successfully address a market need and create value. All players entering the 4G LTE market have unique strategies based on the needs of their respective target markets and business plans. The goal of risk management is to support entities in meeting these business objectives. For the 450 MNOs entering the 4G LTE market in 2013, these objectives are numerous and diverse. A variation in business objectives is likely to result in inconsistent security levels in LTE networks and services offered and a threat to the consistent seamless-roaming service promise of LTE. Examples include:

- **Market protection strategy**—As mobile data traffic volumes increase to unprecedented levels, some MNOs will adopt 4G LTE to alleviate problems of network congestion and bandwidth bottlenecks on their current infrastructure. These MNOs are likely to implement 4G LTE in high-density hot zones, with network upgrades to 4G in phases over the longer term. These deployments are typically multimode operations with 4G in the hot zones where subscribers fall back to lower-speed legacy technologies once outside the zone. Such MNOs are inclined to offer 4G as an extension of their existing 3G networks and introduce security risk as they work through interoperability issues between various access technologies within their own infrastructure and operations. The business objectives of such MNOs focus on subscriber retention rather than acquisition. MNOs in this type of deployment strategy encounter operational, performance and security management issues that are threats to the quality of subscriber experience. Poor service quality can result in MNOs losing their customer base, risking their primary business objective of market protection.

- **First-to-market strategy**—On the other hand, MNOs with the primary objective of speed to market are known to turn up the basic infrastructure and cut corners by deferring deployment of expensive security infrastructure. This approach presents serious security vulnerabilities for the MNO’s operations, partnering MNOs and the subscriber, and can cost the MNO its reputation and its business. Since the security thresholds and risk in each MNO’s business is diverse, MNOs entering peering and partnership agreements to allow seamless mobility to subscribers must be particularly cautious around associated security risk.

BUSINESS MODELS

MNOs develop business models based on business objectives. The 4G LTE architecture and design lend themselves to several new, disruptive models. With each new model come associated challenges, threats and risk:

- **Infrastructure sharing model**—3GPP designed 4G LTE with options for network sharing and continues to evolve it under the TS 23.251 standard. Sharing options include radio access network (RAN) sharing, backhaul sharing and partial to complete core network sharing. Drivers for network sharing range from reduced infrastructure and operating costs and greater geographic coverage, to spectrum sharing, where compelled by regulations or scarcity. Ovum forecasts...
that, by 2015, 30 percent of all LTE networks will involve some form of active network sharing. In network sharing models, MNOs need to consider management protocols for shared resources and load balancing between cells of operators with shared infrastructure. Operations including configuration management, performance management, security management, maintenance and fault management in shared infrastructure bring complexity and operational threats as multiple MNOs need to collaborate efficiently to deliver service. Likewise, rate plans and billing according to usage of shared resources require a level of sophistication to ensure accurate billing to the subscriber and accurate revenue sharing among MNOs. This brings additional layers of risk management requirements.

- **Value added reseller/distributor model**—LTE, through the IP multimedia subsystem (IMS), offers an array of bandwidth-rich applications to subscribers. MNOs who want to move away from the business of solely being broadband pipe providers have the opportunity to partner with application and content providers—positioning themselves as distributors. This includes media content such as video on demand (e.g., Netflix), broadcast video, voice-over LTE and gaming. This business model requires the development of supporting network infrastructure for peering, content and application distribution with quality-of-service (QoS) (i.e., availability, latency, jitter) management. Operating models, revenue sharing, customer relationship management and billing arrangements need to be determined, each bringing its own share of business risk.

- **QoS management**—4G LTE offers voice, data and video convergence with QoS management for each application to ensure appropriate bandwidth allocation and latency requirements. As these services could transit through multiple carriers to get to the subscriber’s device, consistency of QoS through peering points and network elements is critical to maintain service quality. Since many of these bandwidth-guzzling applications have low latency requirements, misconfigured or underprovisioned network elements can cause delays beyond the service tolerance thresholds that result in a poor experience for the subscriber.

- **Traffic management**—Aside from the high-bandwidth user traffic, signalling traffic on LTE is estimated to be 40 percent higher per LTE subscriber than on 3G networks. An inherent vulnerability in 4G LTE is the management of large volumes of user and signalling traffic. If not properly managed via scalable networks and load balancing, signalling floods can cause service degradation and bring the network down, analogous to a denial-of-service (DoS) attack.

**REGIONAL LAWS AND REGULATIONS**

Technologies succeed in the marketplace when they are founded on sound business models. No matter how rich the potential of a technology, business decisions shape the service sets, features and operations of a technology. In turn, no matter how strategic or brilliant the business proposition, legislation and regulations supersede business decisions (figure 3). 4G LTE offers seamless
global roaming to subscribers. In addition, the all-IP service through the IMS can deliver services and applications to the mobile subscriber from various parts of the globe. The global dimension of 4G LTE warrants that MNOs pay particular attention to regional legislation and regulations.

MNOs collect, store, secure and treat subscribers’ personal information under the prevailing local privacy legislation, often pushing legal verbiage to obtain subscriber consent to protect them against potential lawsuits. However, in the global context, there are numerous regions with little to no privacy legislation. Should a subscriber’s personal data from a country where privacy rights are established transfer into regions where there is minimal privacy legislation, the breach in privacy could have serious legal consequences for the MNO. High volumes of data traffic, applications and content on 4G LTE make it more vulnerable than its preceding technologies that primarily carried voice traffic.

Lawful interception (LI) is the process in which an MNO is legally sanctioned to intercept the communication of private individuals or organizations and provide information to law enforcement officials. While 3GPP offers LI-permissive architecture for LTE, its deployment varies in accordance with applicable national or regional laws. In many countries, an LI requires a court order, while in other countries, government surveillance is the norm. To prevent legal violation, MNOs should ensure that their architecture and operations are in accordance with the prevailing regional legislation, keeping in mind that 4G LTE carries over-the-top applications and content globally.

RECOMMENDATIONS FOR MANAGING RISK IN 4G LTE
Risk management is a comprehensive science specific to individual entities and, thus, cannot be detailed completely here; however, there are certain key recommendations pertaining to security risk management in 4G LTE to keep in mind:
• Security should be an integral part of the 4G LTE service launch from the early stages of planning to design and deployment.
• Security architecture and associated security budgets should be earmarked and aligned with business objectives.
• Since 4G LTE involves a myriad of players, a clear understanding of the business strategy and objectives of selected partners in the service chain must be obtained.
• MNOs need to be particularly savvy about articulating security standards to their subscribers as consistency in security levels resides in managing security architectures, parameters and thresholds with partners and service providers in the LTE ecosystem and MNOs do not have unilateral end-to-end control over this.
• In 4G LTE, MNOs should negotiate strong agreements with partners, setting out clear security standards, parameters of interoperations, sharing arrangements and subscriber handover.
• Depending on the operator’s network architecture and peering network arrangements, MNOs should budget for ample interoperability testing, configuration and performance management, considering the seamless technology-agnostic service promise of 4G LTE.
• 4G LTE network architecture and service offerings must be designed in context to a ubiquitous global framework while respecting regional legislation.
• Due to the all-IP converged traffic, 4G LTE networks need to be designed and architected with care toward QoS management. A failure on one service can adversely implicate multiple converged services. Since large volumes of data and signalling traffic are expected on 4G LTE, rapidly scalable networks with load balancing and redundancy are critical.

CONCLUSION
Architecturally robust new wireless technologies, such as 4G LTE, bring enormous service potential to the market; however, they are vulnerable to security threats and risk. If threats from external attackers were not enough, everything from business objectives, business models and network operations to security infrastructure and legislation must be scrutinized by risk management to ensure business success. From the perspective of users (consumers and businesses) who are migrating data traffic to 4G LTE services, inquiring about the MNO’s security standards, business models and operations is a worthwhile pursuit. No matter how advanced the technology, risk management is essential to ensuring security.

AUTHOR’S NOTE
Opinions expressed in this article are the author’s and not necessarily those of her employer.
ACKNOWLEDGMENT

The author would like to thank Tyson Macaulay, vice president global telecommunications strategy, McAfee (Intel), for inspiration, guidance and insights shared.

ENDNOTES