

Publication: Telecomredux
Monthly Unique Users: N/A
Date: 29th October, 2009
URL: <http://www.telecomredux.co.uk/content/view/6443/1/>

telecomredux

Safe and sound



Thursday, 29 October 2009

Arthur Noonan, Omnix Software sales manager (EMEA), discusses the varied safety, security and asset management challenges facing mobile operators around the world...

With mobile communications now an integral part of life the world over, mobile operators have had to adapt to the safety and security challenges of many different markets. While the top priority for operators has always been the safety of workers, customers and the general public, they also face on-going challenges to the security of their equipment and business structures.

As the recession bites, mobile operators are being asked to find even more costs to cut and so are increasingly focussing on how to avoid the expensive pitfalls associated with network safety and security. Careful preparation for these problems, as well as ongoing network planning and monitoring, holds the key to reducing lost revenue and unnecessarily high operational expenditure (OpEx).

Securing the network

While theft and vandalism are challenges operators face in every market, their specific targets can vary wildly. In many African countries the unreliability of the national electricity grid has meant that operators often rely on diesel generators to provide the primary power for base station or other communications sites. However, the generally unstable power supply has also raised the value of power generating equipment, increasing the incidence of generator, diesel and transformer theft. One Omnix customer in Nigeria is currently replacing five to ten generators a month due to theft. In addition, Ahmad Farroukh, ceo of MTN Nigeria, has commented that "all MTN sites are manned by private security agencies, but thefts occur because thieves tend to be adequately armed with ammunition, guns [and] self-loading trucks".

The connection between theft and power supply equipment is continued when considering some of the popular 'green' solutions being offered by innovative vendors. While the marketing and ethical arguments for providing green solutions are convincing, the additional expense of solar and wind powered sources is hard to justify where the likelihood of theft is too great.

Vandalism is also a growing problem in some African communities. Local residents can become unhappy with telecoms operators for paying 'insufficient' site rental, for generating noise pollution or for accidental diesel spillages. Local communities can even become angry that mobile operators do not provide services outside of their remit, such as road construction and community power supplies. Operators have experienced both the intimidation of their site maintenance contractors, as well as the severing of optic fibre cables and the destruction of generators. Nevertheless, many African populations now regard their mobile phones as indispensable (indeed telecoms is often their only reliably functioning utility) and react badly to any drop in the quality of service (QoS). It is imperative then that operators not only respond quickly to site outages, but also ensure they have deployed adequate security to protect both their personnel and equipment, keeping OpEx as low as possible while guaranteeing QoS – attracting new subscribers and decreasing churn.

Another common target of theft, and by no means limited to emerging markets, are the large and expensive copper coaxial feeder cable and components running up the tower sites connecting the base station antennas.

The soaring price of copper has made telecoms infrastructure an ideal target for thieves. Although the price of copper fell during the last few months of 2008 (from over US\$3 a pound to today's price of around US\$2), it remains an attractive target for thieves. British Telecom (BT) has set up its own dedicated squad to clamp down on these thefts, which are estimated to cost the company more than £4mn a year despite the fact that removing live components can put a thief's life at risk. One recent case in the UK saw 27 tonnes of cable being stolen, fetching a total of £35,000.

For mobile operators, as previously mentioned, the expensive coaxial copper feeder cable, acting as a waveguide, connecting either the mobile operator's RF base station or microwave transmission antennas, are often targeted by thieves. But even optic fibre cable links can be damaged if the thieves are under the impression that it is standard copper cabling. For this reason, site planning is essential to ensure that communications sites have all the appropriate security precautions they require: from site fencing to security guards. These types of thefts can create power outages, phone outages and equipment failures. Very often the damage is sufficient to shut down multiple base station, repeater or other communications sites, and the effect can be that customers may even be put in real danger – they might, for example, be unable to call the emergency services.

Although fraud does not directly damage the communications infrastructure of a mobile operator, it is perhaps the most feared form of crime, especially in developed markets. The introduction of regulations such as *Sarbanes-Oxley* in the USA and the *8th Company Law Directive* in Europe, means operators can no longer afford to ignore the need to track all of their resources as accurately as possible. Ceos, Cfos and board members are now more responsible than ever for the accurate representation of corporate assets.

The risks are real: several high-profile corporate accounting scandals in the USA have already shown that inaccuracy can cause the collapse of the affected company's share price. Therefore, as well as any direct financial losses from the activity, operators can stand to lose far more revenue in lost business and regulatory penalties.

Furthermore, the value of a network must be clearly visible and accountable if an operator is trying to attract investors.

In the past, the ability to accurately monitor and report on assets has largely been a question of honesty on the part of network departments within operator organisations. Now it is a matter for board concern that requires integration into financial management processes to drive accuracy and confidence. If assets are left undeclared, or their whereabouts are unknown, penalties can also be enforced for breaches of legislation. It is imperative that network infrastructure is monitored to provide a real-time and realistic view of assets in order to comply with legislation. A framework of activity done (in the form of an audit, for example) ensures companies can prove that no fraudulent transactions have occurred.

Safety in numbers

Although not as high-profile as theft and fraud, health and safety considerations can also create a significant financial burden or risk on mobile operators if they are not planned for in advance. Remedial site upgrades can be extremely expensive and the penalties that may be imposed by regulators for non-compliance are severe.

Operators must consider a myriad of safety regulations during the construction, maintenance and decommissioning of their mobile network infrastructure. As per *The Health and Safety at Work Act 1974*, in the UK for example and its equivalent in other countries, operators have a legal responsibility to ensure that any risks to staff, contractors or the general public are properly controlled. Moreover, any legal claims made by an operator's employees, customers or the general public can result in considerable sums in damages as well as a serious loss of corporate reputation, which will have a direct knock-on effect on a company's revenue.

In the UK, similar to many other countries, *The Corporate Manslaughter and Homicide Act* has created a legal need for organisations to protect their workers. Recent cases have confirmed that directors cannot avoid a charge of neglect by arranging their organisation's business so as to leave them ignorant of circumstances which would trigger their obligation to address health and safety (H&S) breaches. Tracking the location of maintenance workers is one firm step towards this.

In developed markets, base station and other communications sites are put through a rigorous clearance procedure, addressing issues like worker safety, radio interference, aviation safety and the need to minimise the number of sites, towers and other constructions. During the planning of such new sites, operators must consider elements such as anti-climbing defences on communications towers, warning beacons on masts near flight paths, safety railings around rooftop base stations, and compliance with non-ionising radiation legislation (much of which is taking into account public safety fears).

Tower sites in emerging markets often face similar legislation, but more lax enforcement. It is not uncommon for mobile towers in developing countries to be over-loaded with equipment, have non-functioning aircraft warning lights and commit other serious breaches of safety norms.

Even during the planning and construction of sites, operators often fail to carry out quality assurance audits, checking elements like the site's foundation, sufficient wind tolerance and structural integrity. This is essential, given that communications towers consist of more than 10 tons of galvanised iron and many hundreds of components that must be bolted together correctly with the right torque for the tower to remain erect.

In the UK, as in many other countries, the chief problem facing mobile operators is how to ensure compliance with H&S regulations across the huge number of sites on their network. This problem is compounded by the fact that different regions within the UK may have subtly different legislation governing other compliance such as planning restrictions or H&S regulation interpretation. Additionally, site permits and other documentation needs to be renewed on a regular basis.

Thus operators can face an incredibly complex set of requirements and procedures, combined with hefty penalties for non-compliance. Failure to comply with an improvement or prohibition notice carries a fine of up to £20,000, or six months' imprisonment, or both. Unlimited fines and imprisonment can even be imposed by higher courts.

As certified checks and current certificates are generally a legal requirement, it is essential that operators monitor and maintain their own checks and ensure their H&S certification is always up to date.

All this means that operators need to have automated process and planning systems in place to manage their H&S compliance. Given the huge investments made in telecoms networks, it is essential that operators introduce processes to streamline the management of licences, permits, safety checks and the like that are not usually considered with conventional site or estate management systems. It is also vital to support cost-saving activities wherever possible.

These systems should manage the automatic payment of licence fees and the renewal of H&S permits, as well as automatically reminding operators of when site checks are due. Sites must continue to be regularly checked to ensure that they do not later pose a risk to workers or the public, for example through age and corrosion in tower systems and components. These systems can also advise operators on the specific safety considerations for individual types of site (for example: rooftop masts require safety railings). Forward planning can save operators both time and money, as well as protecting them from the risk of heavy penalties.

Solutions

Operators that are proactive about maintaining their assets are the first to benefit from knowing when damaged or stolen technology must be replaced, what it should be replaced with, whether or not the equipment is under warranty, and if the required replacement component is in a warehouse somewhere, waiting to be deployed.

Making sure that existing equipment remains functional and that new equipment is brought 'on-air' as soon as possible also ensures that assets are generating revenue rather than remaining idle. This keeps inventory levels down and leverages real return from fixed assets.

Mobile operators must also track and manage high-value assets across a network in order to ensure they can account for materials such as base-stations and transmission equipment widely dispersed across hundreds, or even thousands of sites. Without such tracking and management, equipment can be stolen or damaged, adding unnecessary costs to the operator and eating into vital revenues.

In addition, without an accurate picture of their infrastructure assets data including for example equipment parameter detail, operators must dispatch a survey team to physically review each site, causing delays and inefficiencies for even minor upgrades or site alterations.

The last line of defence for mobile operators is the insurance claim. Network auditing is essential if operators are to provide an accurate view of their assets in order to secure the best value insurance policy. Vandalism or the theft of equipment from unsecured sites can harm a network to a point that an insurance claim must be made. When insurance companies don't have precise per site equipment asset data for evaluation, insurance brokers underwriting network assets are very likely to overestimate a quotation to ensure it is buffered, as a caution, against the possible true value of the site should a claim be made, which adds an ongoing unnecessary cost to the operator.

On the other hand, if the operator can provide a very precise, computerised record of all its assets, including relevant depreciation, then it will stand in a good position to negotiate a substantial discount from the insurance provider, which might typically represent 10% to 20% of total sites insurance premiums.

While no mobile operator can entirely protect themselves against theft, vandalism or regulatory and legal penalties, the risks can be minimised by efficient project planning, asset management and maintenance tracking. If factors like theft and vandalism are taken into account during the planning stage of a network rollout, asset tracking systems can ensure that masts deployed in high-risk areas have the maximum possible protection. These systems can also ensure that all mast sites receive the safety equipment and certification they require, as well as reminding operators to keep these clearances up to date.

In confronting these challenges, project planning, asset management and maintenance tracking are often overlooked weapons in an operator's arsenal - yet they may also be their most powerful ones.