Safeguard your corporate SIM

By Hein Koen

28 Dec 2015

For companies who have come to rely on SIM cards for machine-to-machine communication and other enterprise-level solutions, fraud can be crippling. Fortunately, there are several preventative measures decision-makers can take to minimise the risk.

©sarella via 123RF

Any company with a sizeable SIM base has experienced fraud in some way - it is one of those things that often gets hidden in the plethora of bills a company receives. We have seen a few cases each totalling well over a R1-million. To say that SIM fraud can put a small company out of business is not an exaggeration.

Abuse categories

There are mainly two types of SIM abuse. The first is spend abuse. As the name suggests, this is when too much money is spent on a SIM card. This can either happen as a result of a device becoming faulty or a person using too much data. Often, this is written off as legitimate spend incurred during the course of business.

The second, and more concerning one, is when SIMs are stolen or compromised. These SIMs, typically found in terminals or point-of-sale devices, are then used for WASP-type services like buying airtime and data using the corporate account. With syndicates using sophisticated methods to do this, the financial implications on a business can quickly become serious.

So what are some of the steps one can take to help combat SIM card fraud in the organisation?

Check your SIM

As a first step, the business needs to ensure that the correct SIM is in a device. In other words, the SIM has to be risk managed. Ideally, companies should not use open-ended post-paid SIMs but opt to go the prepaid route. This massively reduces the potential for bill shock.

With prepaid SIMs, companies can manage their costs in real-time. After all, a prepaid SIM can only use the amount of airtime or data loaded on to it. This provides decision-makers with a much more efficient way of managing the associated

costs. There is also no way that out of bundle rates, especially when it comes to mobile data, escalate out of control.

Use management tools

Companies should also evaluate whether they have the tools in place to manage their SIM cards effectively. There are online tools available to take the hassle out of managing prepaid SIMs and devices in real time.

However, working with a trusted service provider who has the expertise and know-how to do it means an organisation can focus on meeting its core business deliverables.

Keep devices locked

Another very useful measure to take is for decision-makers to lock down their devices in the field. There is software that can do this, either on a firmware or device level. With a mobile workforce using tablets and smartphones, such software can be used to minimise risk even further.

One of the best things about going the prepaid route is that businesses need not worry about performing SIM swaps when devices are lost. It is just a case of inserting a new prepaid SIM into the device as the SIM is not linked to a specific account.

At the end of the day, it can cost a lot of money when falling prey to SIM fraud and abuse. By implementing some of these proactive measures, companies can mitigate some risks and monthly bill shocks.

ABOUT HEIN KOEN

Co-founder and Director of Flickswitch, a technology company in the mobile telecoms space focusing on the management of M2M data SIM cards across various African mobile networks. He is passionate about mobile data and its connectivity means in Africa. As the use of data SIM cards increases in this age of IoT (Internet of Things), it needs to be managed. The intersection of data SIM cards and effectively managing it on a large scale, is what gets Hein excited.

- Safeguard your corporate SIM - 28 Dec 2015

View my profile and articles...