Corporates using cellphone technology to enhance security

South African corporates are increasingly tapping in to sophisticated mobile forensic technology to boost security within their organisations, according to Adam Victor, MD of Pandacom Distribution.

Image: www.freedigitalphotos.net

The technology enables forensic investigators to extract contact lists, pictures, videos, SMS and instant messages, as well as call histories - even if they have been deleted - from any mobile devices and SIM cards.

However, this technology cannot be used to hack into cellphones in the same way that the UK's The News of the World journalists "eavesdropped" on the private conversations of celebrities and royalty. What it can do is identify when a cellphone is being hacked.

"Developed by Cellebrite Mobile Forensics, it can only be used on cellphones that are physically in the hands of the investigator," Victor said.

The technology is proving hugely successful in combating incidence of industrial espionage, insider trading, corruption and other white collar crimes within organisations. By checking corporate cellphones regularly - in much the same way as many security-conscious organisations monitor emails and internet browsing patterns, corporates could potentially identify suspicious employee behaviour.

The rapid spread of smartphone Trojans

"At the same time, the rapid spread of smartphone Trojans makes many corporate executives' phones vulnerable. These Trojans can clone SIM cards - leading to identity theft and fraud, allow text messages to be read, send premium-rate SMS messages, steal location information gathered by GPS and Wi-Fi - and even record phone calls and text messages.

"Imagine what would happen if executives discuss highly confidential information on their cellphones, the conversation is

secretly recorded and sent to a remote site, without anyone knowing.

"As a result, many companies now routinely used forensic mobile tools to scan executives' phones for Trojans and other viruses," Victor said.

Similar mobile forensic technology is being used by crime enforcement agencies around the world - including South Africa - to solve a wide range of crimes.

Crimes involving syndicates

There are many examples of crimes involving syndicates that have been solved using this technology. Once the law enforcement agency is able to obtain just one of the phones used by a syndicate member, it can be used to unlock the details of past and potential future crimes, as well as to identify other syndicate members.

One might think criminals would be careful about the information they send via text messages, but it appears that this is seldom so.

In a recent spate of housebreakings in Los Angeles, for example, police were able to identify a suspect's accomplices, determine the suspect's location at the time as the various crimes were committed, and even obtain an "inventory" of items that had been stolen - as well as their value.

In another case in Canada, a suspect smashed his cellphone when he realised the police were going to confiscate it - but to no avail.

"Although the phone was damaged beyond repair, the forensic investigator was able to extract data from the SIM card - and this helped to convict the suspect," Victor said.

In England, the technology has been used to strengthen cases against members of paedophile rings, who often go to great lengths to protect each other. The technology was used to tie together the various strands of the rings by comparing text messages and instant messaging chats as well as call logs and contacts found on one suspect's handsets with data found on victims' or other suspects' phones.

"The availability of this technology in South Africa considerably strengthens the capability and capacity of our law enforcement agencies. At the same time, the corporate sector must take the risk of cellphone-related crime far more seriously than they do at present - and then take proactive steps to protect themselves," Victor concluded.