

COMPUSAFE

electronic asset security



Get proactive, not reactive!

Brad Nathanson Investigations - 0832502 007

Bouvest 2383cc T/A Compusafe
P.O.Box 2112, Hillcrest, 3650, Kzn
Reg.no 2002/071148/23
Vat no: 4710203334
Office: +2731 765 3153
Fax: 0880317653153
Email: info@compusafe.co.za
Web: www.compusafe.co.za
Ian Colls – 082 4519338
SACAN- 0861-623-646
SAPS - 10111

Report on computer theft in South Africa

The theft of computers from businesses in South Africa has over the last 7 years emerged as the leading non-violent crime against our business community, having in the last 5 years cost the business sector more than armed robberies and cash in transit heists combined. To fully understand the dynamics of this crime, one needs to look at the fact surrounding legislation, or should I say the lack thereof when it comes to industrial espionage, using intellectual property as evidence in the South African judicial system, the demand and market for stolen IT equipment, the responsibility of the security industry to the public when taking a pro-active stance regarding a reactive policy, the SAPS' roll and responsibility, and how the government and SARS are benefitting from this crime.

The crime of computer theft is syndicated crime and involves a well organized network of criminals, hence the term "organized crime". The syndicate involves the use of illegal immigrants from across our borders to do the actual breakins, so that if caught, deportation is an option to escape prosecution. The breakins are well planned with information gathered prior to the crime; information such as addresses, the security company monitoring the premises, the telephone network system and which lines are used for the response of an alarm activation, opening and closing signals, self-test signals, change of shift times for reaction staff, and most importantly whether the company is using ADSL. The gathering of this information will be explained in more detail further on in this report. We are dealing with big players with more operating funds at their disposal than we have in the budget to fight crime. Their business runs at a 100% profit margin, and they obviously have an ongoing demand for their stolen goods. They are well educated in the legal system and know how to work around it, and have intricate knowledge of telecommunication systems, alarm and security systems and how to either bypass the technology or simply work within its parameters. Simply put, if you study something for long enough you will eventually become an expert in that field, whether you are using those expertise to fight crime or commit crime.

Currently in South Africa there is no legislation for the prosecution of theft of information, as information is classed as intellectual property and in this country may not be logged into evidence unless it is registered intellectual property, as is the case with Microsoft who can prosecute illegal use of pirated software. If a stolen computer is recovered, usually with the bar-coded serial number removed, the only other way to identify the legitimate owner is by the information stored on the hard drive. This information is however not admissible and the case is almost impossible to prosecute. Until legislation surrounding this act is changed, the syndicates are able to continue with their business with little fear of recourse.

The security industry in South Africa mainly offers a re-active service of monitoring and response, leaving the pro-active responsibility on the SAPS, the insurance industry and the public themselves. Security companies have legal contracts with their clients clearly identifying their roll in the services that they provide and the conditions of that service. A decade ago alarm systems were very effective as deterrents to breakins, but over time have become almost ineffective when dealing with this syndicate, and merely act as a loss damage service and a notification that there has been a breakin for insurance purposes. The truth is that alarm systems do not stop breakins, we all have alarm systems in our businesses and theft statistics clearly show that business breakins increase annually. The level of technology in the design of alarm systems used in South Africa is way below the standard compared to countries such as America, Canada, and the EEC. The reason for this is very simple – the manufacturers of alarm systems in this country will only invest in what the public are prepared to pay for, usually the cheapest system available to keep their insurance company happy and meet the minimum requirements to get insurance cover. The recommended investment on security for businesses in South Africa is 5% of budget, a figure that across the board only big corporate can afford, leaving the majority of the business community well below standard and opening themselves up for crime, a fact that the syndicates are well aware of and take full advantage of.

If one looks at the roll of the SAPS in the prevention of computer theft, one must understand the problem within the SAPS as far as mandate goes. Crimes are categorized according to the degree of violence, the safety of the public first: murder, attempted murder, rape, child abuse, armed robbery, etc with theft of computers, especially considering the stolen goods are covered by insurance and that the crime involves little public contact, except for the odd security guard beaten or even killed for resisting, this crime is at the bottom of the priorities list. The average SAPS investigator has more cases than he can cope with, the problem of understaffing in the SAPS, and the absence of a specialized task force to investigate this crime, all contribute to the poor result in prevention. Taking these factors into consideration, and trying to understand the dynamics of who the responsibility of preventing this crime really falls on, one can fully understand the frustration of the public when it seems like nothing is being done to curb this crime. The public's frustration is not without cause, however I do believe that the public are grossly misinformed when it comes to this crime and what we are truly dealing with, the problems we in the security industry are facing, and without the correct information at hand, are in the dark and can not make the correct decisions when planning and budgeting for matters of security.

The security industry in South Africa has been the fastest growing and one of the most profitable industries over the last decade. The security industry in general provides the public with product, solutions, and a service for which they profit. What is of concern is how our government is also profiting in the way of revenue through vat collected on firstly the services rendered by security companies, but more importantly through vat collected on replaced stolen goods through the insurance industry. This may not at first seem like much of a concern, but when you do the figures on how many homes and businesses have alarm systems with a response service, and the total claims nationally on IT theft, motor vehicle theft, etc the profitability of crime in South Africa takes on a new perspective. As long as our government is collecting these funds, I do not see a reason for them to want this crime to stop; simply a mathematical fact!

Investigation on Telkom influence in computer theft

We have for many years underestimated the public in solving crime, but I have found that it is the public that have been so instrumental in my investigations on computer theft in South Africa. The public are like innocent children and say it as they see it, and without even knowing it, have led me in a direction in my investigations that at first may seem far fetched, but to date no one or anyone in the security industry has challenged my findings or proven otherwise.

One common denominator has over the last 7 years of investigations has been the influence of Telkom in the syndicate responsible for computer theft in our country. Once one realizes that we are dealing with organized crime and that the syndicate is using the very same technology we implement to protect ourselves, against us, then one can start to deal with the problem. Alarm systems are reliant on having a communication link between the alarm and the security company in order for monitoring and reporting events and activations, in the majority of the time the fax line. The industry is slowly catching up and the introduction and implementation of radio transmitters as a backup communication link to the security company is starting to make a difference, however the primary solution is still the use of telephone lines, which in my opinion is the weakest link in the system. If a security company can not receive a signal of a positive breakin it can not respond and the system has failed.

My investigations show, that on the Telkom database, primarily the commercial data base, there is all the information available that this syndicate would need to be as successful as they are at committing this crime in such a well orchestrated manner. This data base offers: the security company monitoring the business, the telephone line/s used for linking the alarm to the security company, the opening and closing signals, the self test signals, whether the alarm has been armed or not, and whether computers are being used in that company through the presence of an ADSL line. All this information in the wrong hands is resulting in what we are experiencing at present with this crime, and how it is almost impossible to stop.

The ADSL line in particular is the key factor in breakins and here are the facts:

- 1) A company, whether run from a factory, commercial sector, or home based, that installs ADSL usually experiences a breakin with the first 3 weeks of the instillation of this line.
- 2) The same can be said for a business that relocates to new premises and has this line transferred.
- 3) The syndicate make a point of stealing the ADSL server, initially believed to for its level entry, but now we know it is primarily for the syndicate to monitor when the stolen computers have been replaced.
- 4) When the ADSL server is stolen during a breakin, a repeat breakin usually takes place within a week, but cases have been reported within 24 hours.
- 5) When the ADSL sever is not stolen during a breakin, a repeat breakin usually takes place 10 to 14 days later.
- 6) Many companies have experienced faults with their ADSL lines and more importantly with their fax line/s just prior to a breakin, remembering that alarm systems communicate via the fax line.
- 7) Companies with ADSL experience more breakins than companies using wireless networks such as 3G.

In South Africa, there is only one service provider that supports ADSL – Telkom. There is only one service provider that has all this information at hand, and who can monitor

telephone lines 24 hours a day. Further to my investigations, I believe that the fax lines are being suspended during breakins for a limited period of time. This allows the thieves to enter the premises and take their time in choosing the IT equipment they want, normally the newer equipment, and leave within a period of time before the line is unsuspended, by which time the thieves are long gone. Make no mistake, the alarm does activate and tries to contact the security control room, but can not until the line is re-opened. The time that the breakin occurred and the time that the security company get a signal are not always the same time. This theory would clearly answer the questions so often asked, and how companies have lost all their IT equipment in one breakin, in some cases entire floors of computers.

- 1) How did the thieves manage to steal all this IT equipment in such a short period of time, 3 to 7 minutes, when it is evident that they had more time available ?
- 2) Why is it when the security reaction staff arrive at the scene in what seems to be good time, the thieves are long gone?
- 3) Why was the theft done in what appears to be a very neat and selective manner, with the computer cables not cut or torn out, but carefully removed?

This is I believe the latest method of bypassing the telephone line link between alarm and security company. In the past, and still used today, it was as simple as cutting the line, removing the line from the junction box for which you would need the Telkom junction box diagrams, keeping the fax line engaged during the breakin, or diverting the line away from the security company which could be done from the Telkom exchange. It has become harder for the syndicate to use these older methods as the design of alarm systems has caught up and changes have been made to deal with these problems.

Enter a radio transmitter connected to the alarm into the equation, and we have an entirely different result. If the radio transmitter is installed correctly and the alarm configured correctly with the radio on dual response, then the breakins are "smash and grabs". The time that the thieves have is drastically reduced as the security company is almost guaranteed a signal from the alarm. This is when we start to see rush jobs, wires torn and cut, and in many cases only the ground floor effected in multi-storied buildings, and the computers closest to the point of entry stolen.

The sad reality is that either way, the alarms do not stop the breakins from taking place, the correct configuration of the alarm system merely dictates the amount of loss per breakin. The more we upgrade the alarm systems and design thereof, the more innovative the syndicates become, and the more violent they become in their approach. Keeping security guards on site does help to a degree, but statistics clearly show an increase in security guards been intimidated, beaten, and even killed. Further more, the syndicate are resorting more and more to daylight armed robberies for IT equipment, and then returning about 10 to 14 days later at night for a repeat breakin.

Where are the stolen computers going?

The big question! There has to be logical answer, and I believe we have been looking in the wrong place all along, when the most simple explanation is usually the correct one. Some believe the computers are going overseas to the UK, America, etc. In reality when a new entry level computer is brought into the market, the redundant stock is dumped on 3rd world countries like South Africa, so why would they want them back. Another theory is that they are going into Africa and neighboring states. Possible, but bear in mind that the rest of Africa is still very far behind technology wise and does not

have the infrastructure to support this kind of technology, let alone the funds. Some believe the stolen computers are going to second hand shops, but considering the sheer number of computers stolen, these outlets would never be able to cope with the numbers, and it is now policy for these outlets to record the details of anyone trying to sell secondhand electronic goods. Then there is the theory that students in tertiary education are buying them as a student without a computer is seriously disadvantaged. I could agree that a small number of these computers could land up in the hands of students, but they would be specialized computers such as Apple Macs for design students. It is my opinion that the computers are not crossing our borders, but are staying right here in South Africa. I believe that they are being rebuilt and sold to the Department of Education under tender process for less advantaged schools. These computers have to be moved in bulk, considering the sheer numbers, and schools need plenty of them. To date no one has challenged the origin of where the Department of Education gets their computers from or who is filling these tenders. I also believe that the funds needed for purchasing these computers are coming from the revenue collected in vat on the replacements through the insurance industry, about R450 per computer – if not, why not!

Conclusion

The future of the security industry and the success there of will eventually come down to ethics. Every man has them, but not every man has prioritized them correctly. It is a sad day in our country when you look into the eyes of the public and you can see the lack of confidence, the frustration of questions that are not being answered, the growing mistrust, the fading hope in the solutions promised, and desensitization of crime and how the man on the street has come to accept the ongoing high levels of crime as an every day part of South African life. The privatization of security in our country is a clear example of how our government can not cope with the increasing levels of crime, and how the public have had no choice but to find their own solutions by turning to privatized security companies to protect us. This in itself will self destruct if the security industry does not deliver the results that the public are demanding, and it is the public themselves that will eventually bring this about. We need to start honest with the public and admit that we are dealing with a virus that is mutating faster than we can create antibodies to fight this infection. Maybe when we can face up to the realities of the problem and start putting the community before profit margins, then maybe we will win back their trust and faith and real change can start to take place. I believe it's about taking responsibility and liability for a service that we supply to the public, and starting to listen to their needs and not that of politicians with 24 hour protection. What concerns me the most, is that my findings from this investigation have been provided to the major security companies, some of which have responded by informing me that it is not their problem as they sell a reactive service and not a pro-active service to the public, and to the SAPS who have never done anything with the information provided.

The purpose of this report is not to discredit those in power and the security industry as a whole, but rather to bring to light the issue of who's responsibility it actually is to make effective change. We can not continue to keep passing the buck from government, to the SAPS, to the private security sector, and to the public. In reality we are all responsible and all have a part to play if anything is ever to be done about crime in our country. It brings to mind Proverbs 28:5 – translated it says that an evil man will turn a blind eye for his own benefit – usually financial!