

SEPTEMBER 2011

INFORMATION UPDATE:

The following information reflects the lists handled for September 2011:

Dräger

Lists: 4
Records: 1485
Hits: 673

Tracker:

Lists: 12
Records: 291
Hits: 84

SAPS 13

Lists: 17
Records: 261
Hits: 65

Enquiries

Enquiries: 81

INSIDE THIS ISSUE...

SAICB UPDATE	1
FRAUDLINE	1
INFORMATION UPDATE	1
ARTICLE—SERVAMUS	3
ARTICLE—ICSA LABS	8
ARTICLE—WHO	9
CONTACT	7

SAICB UPDATE

SAICB UPDATE

The release of the National Crime statistics by Minister of Police, EN Mthethwa, on 8 September 2011 has further entrenched the SAICB as the go to organisation for information on the crime and fraud situation in the short term insurance industry with the Minister referring to information supplied by the SAICB on two issues—the decrease in house robberies and the decrease in car hijackings noted in the stats.

The close working relationship the SAICB has with the South African Police (SAP) and National Prosecuting Authority (NPA) in addressing the crime and fraud situation in the short term industry has led to several successful projects including the following:

Operation “Facelift”

On 21 September 2001, Operation “Facelift”, a joint SAICB and SAP project arrested 9 members of a fraud syndicate operating in KwaZulu Natal.

The five month investigation by the SAICB and its members, with the assistance of the SAP and the NPA, uncovered the syndicate operating in Escort and Phoenix involving several members of the same family.

The Modus Operandi used is as follows: The suspects bought vehicles from salvage yards, vehicles were registered in the names of other members of the syndicate to create a record for the vehicle. The vehicles were not roadworthy but were registered with the assistance of corrupt officials. Vehicles were then insured at multiple insurers (SAICB members), and accidents were staged with syndicate members, and multiple claims lodged. The value of loss for the industry is approximately R2 million.

This case is the ninth case that the SAICB has successfully brought to court with the assistance of the SAP and NPA. All previous cases were successfully prosecuted with sentences ranging from fines to jail terms.

FRAUDLINE

In August 2011, 26 reports were received of which 20 reports were for the short term insurance industry, 0 report was received for Brokers and 6 reports for the life industry.

Since 2002, 27141 reports have been received of which 923 reports were for the short term industry 136 reports for the brokers and 372 reports were for the life industry.

For further information on the statistics, please contact Melanie Pillay on melaniep@saicb.co.za



0860 002526
insurance@fraudline.co.za

MEMBERS

SANTAM
 MUTUAL & FEDERAL
 HOLLARD
 LION OF AFRICA
 REGENT
 TELESURE
 ABSA INSURANCE
 STANDARD BANK
 INSURANCE
 OUTSURANCE
 MOMENTUM
 MIWAY
 ALEXANDER
 FORBES

PARTNERS

SOUTH AFRICAN
 INSURANCE
 ASSOCIATION (SAIA)
 TRANSUNION
 FRAUDLINE
 MEMEX
 SAFPS
 UNICODE
 BACSA
 NEWORDER
 DATADOT
 CGC
 SAVRALA

SAICB UPDATE *cont...*

Operation "Ghost"

This case mentioned in the last two newsletters came before court on 28 September 2011 again and was postponed to 24 November 2011, because the accused applied for legal aid.

Empangeni Pound Project

From 9 to 14 October, the SAICB, its member representatives and a project team from the SAP will initiate a project to address the vehicles being held for safe keeping in the police pounds in the Empangeni area.

The objective of the operation is to identify and dispose of ± 700 vehicles that are currently under safeguarding at the different Police Stations in the Empangeni VISS policing area.

Fifteen (15) people from the insurance industry confirmed their participation for this operation that will take place at 22 police precincts on the Kwa-Zulu Natal North Coast. The duties of the insurance industry personnel will entail the following:

- To capture details of all vehicles in safeguarding.
- To establish ownership of the vehicles in safeguarding. (Both insured and uninsured through ITC and other systems available to the insurance industry.)
- To assist the SAP in notifying the rightful owner about the recovery of the vehicle.

The SAP will provide twelve members that will assist the insurance industry in the identifying of vehicles and the administration process surrounding the disposal of the identified vehicles.

This project will follow the project to be launched on 3 October 2011 at the van Rijn Deep pound in Gauteng where ± 2000 vehicles are housed. This project will run from 3 to 7 October 2011.

Reports of the Empangeni and van Rijn Deep Pounds will appear in the next issues.

Isipingo Pound Project Update

These two projects have been initiated after the very successful intervention by the SAICB in the Isipingo Pound in KwaZulu Natal resulting in a saving for insured and uninsured vehicle owners and insurers of approximately R30 million. The Isipingo project included visits by representatives from the insurance industry to the pounds and lists sent by the personnel at the pound over a period of a year—from August 2010 to August 2011. Colonel Dlamini and especially Capt Heneke need to be commended for their continued support and allocation of resources to these projects.

Regional Court Judgement

The case before the Regional Court in Wynberg in Cape Town regarding the use of the Dräger breathalyser has been finalised with the judgement delivered on 9 September 2011. The judge refers negatively to certification, calibration, maintenance, administration, equip

SAICB UPDATE CONT...

ment, training (not sufficient), training manual (confusing), non-testing of the specific Dräger Model, accreditation, etc.

The outcome indicated that while the Dräger breathalyser can be used for enforcement of the legal alcohol limits for drivers, the device has to be certified, calibrated properly accordingly to the law of the country and the personnel using the device have to be properly trained in the use of the specific device and model being used. The full judgement is available on our website: www.saicb.co.za

FOR FURTHER INFORMATION PLEASE CONTACT MELANIE PILLAY ON melaniep@saicb.co.za OR HUGO VAN ZYL ON hugovz@saicb.co.za

ARTICLE— SERVAMUS

MICRODOTTING

- New technology for a new breed of criminal

By Herman van Zyl

Many of us remember the good old days when, in terms of criminal tendencies, criminals had the "decency" to wait for you to leave your home or car before going about their business. The majority of criminal attacks took place in your absence, resulting in a nasty surprise when arriving home or in the parking lot, such as being greeted by a broken window or an empty parking bay. Shock and frustration follow when you realise that your house has been broken into or your car has been stolen, but at least you would seldom get severe trauma, injury and death as part of the package. A few phone calls to the police, insurance broker and maintenance companies would sort out the majority of one's problems, and soon one would be able to continue with a normal life.

Modern trends

Sadly, things have taken a turn for the worse. Armed robbery has increasingly become the preferred option for criminals to source what they want. Nowadays, an array of visible security measures such as high walls, all-round security gates and burglar proofing too often seems to serve the sole purpose of attracting criminals, due to their perception that the owner is hiding highly sought-after valuables on the inside. The added security result with this new breed of criminals - against whom we are often almost defenceless, and who deliberately wait for owners to return home before launching their attack - is that they are ruthless, unable to feel remorse, and treat victims with unthinkable violence and cruelty.

So-called property crime increasingly takes place in the presence of the owner/legal possessor of the property. All too easily, what started as a "mere" property crime can end up becoming a contact crime, often with irreversible consequences. Daily reports about street, house and business robberies, hijackings and farm attacks make these crimes seem like a never-ending onslaught and nightmare. At the very least, the victim suffers severe trauma.

How well are we protected?

How effective are our current security methods against this type of criminal attack? The short answer is that, in many cases, they are pretty much useless. The principle on which almost all current security methods are based is the principle of time delay. Security devices are supposed to limit the amount of time that the criminal has to commit the crime - the longer the delay, the more effective the device, and the safer we are, often resulting in the attacker turning and running away.

Anti-theft devices have no effect when a gun is put to the victim's head. All the time bought by expensive devices is neutral-

ARTICLE— SERVAMUS CONT...

ised in an instant. Furthermore, it serves no purpose to spend more money on more of the same: higher walls and more electric fencing will get us nowhere. We need to start thinking in a new direction to ensure the safety of communities and the protection of valuables.

A new strategy is critical

It may prove fruitful to have a better understanding of the way crime syndicates set up their environment to best suit their activities. Generally speaking, criminals need a super-quick procedure to acquire goods of value and to convert those goods into cash. This procedure must be riddled with escape routes in case something goes wrong. This will allow the perpetrator to walk away, avoiding arrest or (at the very least) not being found guilty in a court of law. We can consider these basic requirements for an effective criminal acquisition and disposal process. But what if we were able to seriously compromise typical criminal procedures?

Microdot technology may have a capacity that can easily be overlooked, as the majority of people who have been exposed to this technology perceive it merely as a system which enables authorities to return lost property to its lawful owners. Insured owners in particular often do not want their property back - they prefer to get paid out and buy new property. Short-term insurers, on the other hand, prefer to budget for a certain projected loss rate and set monthly payments accordingly to ensure annual profit. The recovery of property that has already been paid out for is viewed as a bonus and, at best, it is utilised to quote more competitive monthly insurance premiums where required. Thus, insurers are also not keen on the microdot system. Despite all this lukewarmness towards microdot technology, security experts around the world agree that in terms of cost, ease of application and effectiveness, this system has the best potential to bring down crime levels significantly and permanently. Several South African cases have been documented wherein microdot technology, in these cases the services of DataDot, became involved in crime prevention projects with astonishing results.

What can be expected from this amazing forensic technology?

Some of the benefits are that:

- Robbed and stolen items stay traceable and identifiable even under extreme conditions.
- The technology creates doubt in the criminal mind, because it doesn't involve just a single device.
- Marked items can often place the person found in possession on the scene of the crime.
- Being found in possession of stolen property marked with microdots complicates efforts to give a reasonable explanation of how you had come into possession of it - which creates an added chance of arrest.
- It often provides a starting point for an investigation, reducing the number of dockets that are closed without meaningful investigation.
- It is likely to provide an early breakthrough in the investigation, thereby easing the load on detectives.
- The involvement of microdot technology can improve the quality of dockets that are sent to court, making life easier for prosecutors.
- It can be instrumental in exposing corrupt government officials who either fail to check for property found in suspicious circumstances, or who do not follow up on alibis properly.

When applied correctly and policed correctly, microdot technology is a formidable weapon against any form of property crime, regardless of the method of acquisition preferred by the perpetrator.

Consider the fact that criminals usually prepare for an attack and assess the circumstances surrounding the area of the intended attack. For example, they need to know the movements of a potential victim, what they can expect to source, how many people reside in an identified residence and what the security measures are on the property. Criminals are known to create "briefing sessions" where liquor is supplied free of charge on Fridays and Saturdays at predetermined locations. Do-

ARTICLE— SERVAMUS CONT...

mestic workers and gardeners, mostly unintentionally, disseminate the security information required by criminals during such sessions, often because they are "under the influence" and talk easily. In one reported case, certain high schoolchildren were targeted whilst parents went away for the weekend. Think of the benefits that can be had where the domestic workers of an entire residential area can be exposed to the implementation process of a microdot project. The news will most certainly spread.

Also, ideally for the criminal, crime takes place in an environment that is insufficiently controlled, but once proper control is brought into any area, the crime rate usually drops. However, this is often easier said than done. Microdot technology provides a means to bringing sustainable control into a community. It does not need large numbers of personnel or expensive resources, and is therefore also an option for poorer communities. It will continue to be effective for years, and only needs the occasional small update.

The strength of the system is two-fold: Firstly, in terms of the sheer numbers of microdots used - for example, in the case of a vehicle, up to 10 000 microdots are involved. Criminals have almost everything in their favour, but one thing they don't have is time. To deal with 10 000 microdots can take an awful amount of time. Secondly, there is the element of uncertainty. A criminal will never have a guarantee that s/he has removed all the microdots. The advantage is that the authorities only have to find a single dot.

No matter what we get involved in, we want to know where we are heading. If there are too many unknown factors, we would rather avoid it. Criminals are no different.

Can the microdot system be successfully implemented in a community?

Together with Datadot Technologies South Africa, a Southern Cape-based company, Bothasig Police Station in the Western Cape launched a project which has since been accepted as a best practice in the station's precinct. Residences where Data-dot has been implemented were not targeted by criminals for the best part of six months. Purposefully, the project was started in the most problematic sectors of the station area.

Each phase in the project can be explained in more detail as follows:

1. Mobilisation

- Share the vision
- Get people excited about the fact that a substantial and permanent reduction of crime in their community is within their reach
- Stress the importance of standing up against crime together, as a community
- Identify key role-players, including volunteers that are willing to assist with the implementation.

2. Communication

- Set up a communication network within the project area
- Communicate and explain the concept widely and clearly to people on both sides of the law (criminals can be informed in detail, because there are no quick fixes for microdotting)
- Communicate the cost per household
- Invite home owners within the project area to indicate their interest in becoming part of the project and have their valuables marked.

ARTICLE— SERVAMUS CONT...

3. Introduction

- Make first contact with the home owner
- Give a quick run-down of the project
- Do a demo fitment of one or two items, to make sure that the home owner understands the DIY procedure (if the neighbourhood watch/community safety initiative members, reservists and volunteers are involved, this phase is easier).

4. Registration

This is the minor administrative function of collecting completed documentation and faxing it off to ensure that the relevant details are uploaded onto the Datadot database. One person, functioning as part of the coordinating team, can easily manage this task.

5. Follow-up

- Have a second contact session with the home owner
- Gather feedback about results and the progress of the project, as well as checking on the impact on crime statistics
- Conduct quality control on items already marked
- Enquire whether further items were indeed marked
- Ensure that the warning board is displayed in a suitable position
- Render assistance/advice as may be required.

6. Incident Response

(this is mainly a SAPS function)

- Determine the SOP (Standing Operating Procedure) beforehand in consultation with and to the satisfaction of all role-players/ home owners
- Ensure immediate response by the SAPS according to SOP once an incident takes place at a Datadot home
- Give feedback about the outcome of the response to the home owner
- Adjust the SOP if necessary.

Central coordinating team

Any project needs a project leader with a few pairs of hands to give assistance. Communities need somebody who has a passion and a need to serve as project manager. A chairperson of the neighbourhood watch may be a good candidate, while the SAPS sector manager can act as an assistant. A project to substantially reduce crime within a community will not happen by itself - it will have to be driven! This is the function of the coordinating team.

Unexpected benefits

Some of the unexpected benefits to be gained from such a project may include that:

- The community and their local police will move much closer together
- Trust in the SAPS that has been damaged can be restored
- Local police will have a renewed sense of drive and energy to tackle the task at hand with vigour and enthusiasm

ARTICLE— SERVAMUS CONT...

- The community which has learned not to function as a community can rediscover the art of functioning together as a community and reap the benefits, such as a drop in crime levels.

What are microdots?

Microdots are tiny polyester particles that are inscribed with unique information. Each microdot is no larger than 1 mm in diameter. If an owner chooses to apply microdots to his/her vehicle, 10 000 of these microdots can be applied throughout the vehicle using a special adhesive. The information etched onto the microdots relates exclusively to the identity of a specific vehicle. The water-based adhesive used contains UV additives, providing easy identification of sprayed areas. The microdots are sprayed onto a minimum of 80 sites within the vehicle, making it difficult for would-be thieves to alter the vehicle's identity. The sheer number of dots, both in overt (30%) and covert (70%) locations, effectively provides the vehicle with its own DNA. The dots are only legible under a low-powered microscope or by using a special UV light, making it difficult to determine exactly where they have been placed.

Similarly, microdots are applied to office and household equipment to provide them with their own DNA. Once they have been recovered by the police after a robbery or burglary, the police will be able to positively link the equipment with its legal owner.

Any household, office or electronic item can be microdotted including cellphones, DVD players, personal computers, digital cameras, quad bikes, jet ski's, laptops and other personal valuables, and linked to DataDot's exclusive micro asset tracking database. Client details are linked to each individual PIN, and each unique PIN is registered on the Micro Asset Tracking SA national database. Even jewellery and watches can be marked with metal dots, as these items have become favourites among criminals.

Source:

Kempen, A. 2009. "Small dots ... big help to fight crime." **SERVAMUS** Community-based Safety and Security Magazine. October.

(See related articles about microdotting and DataDot in **SERVAMUS**: April 2008 and August 2009.)

ARTICLE COURTESY OF SERVAMUS COMMUNITY-BASED SAFETY & SECURITY MAGAZINE. ARTICLE ORIGINALLY PUBLISHED IN SERVAMUS: SEPTEMBER 2011. FOR MORE INFORMATION PLEASE CONTACT (012) 345 660

CONTACT

For further information or if you wish to reproduce any of the articles in this Newsletter, please contact :

Hugo van Zyl on hugovz@saicb.co.za or Melanie Pillay on melaniep@saicb.co.za

ARTICLE— ICOSA LABS

ICOSA LABS OFFERS TIPS TO COMBAT GROWING MOBILE SECURITY THREATS

Warns Users to Only Access Trusted App Stores, Think Twice About Accepting 'Permissions'

MECHANICSBURG, Pa. – Security risks to mobile devices continue to rise as hackers discover new ways to infiltrate smartphones and tablets, especially by exploiting mobile applications.

“Today users face daily threats from Trojans and other computer viruses that can potentially expose sensitive personal data, including credit card numbers,” said Andy Hayter, anti-malcode program manager for ICOSA Labs, an independent division of Verizon. “In addition, undetected Trojans can lead to expensive charges on customer phone bills by sending text messages and making calls.”

To combat mobile security risks aimed at smartphones, tablets and apps, ICOSA Labs offers seven tips to help business and consumer users protect themselves:

1. Only buy apps from recognized app stores. Apps from unofficial third-party stores and applications downloaded from peer-to-peer sites are much more likely to contain malware than apps sanctioned by official vendor stores such as the Android App Market or Apple App Store.
2. Think twice about accepting “permissions.” Most applications, legitimate as well as malicious ones, require users to accept several “permissions” before the apps are installed. Check carefully to be sure that the app comes from a legitimate source.
3. Monitor bills for irregular charges. If attackers gain access to personal information stored on your phone, they can quickly rack up charges by sending “silent” text messages to high-priced call services. For example, if the Android Trojan GGTracker is inadvertently installed on a device, it can sign up users, without their knowledge, for premium text messaging services.
4. Employ security policies to protect employer-issued devices. Employers should enforce password-based access and require voice mail codes so that only authorized users can access data on employer-issued devices.
5. Be mindful that more and more employees bring their personal devices to work. Companies therefore must have security systems and policies in place to safeguard their business environment and prevent access to company networks from employees’ personal devices.
6. Remember that mobile devices are tiny handheld PCs. Many security threats that apply to traditional computers also apply to mobile devices, such as smartphones and tablets, and consumers should take necessary measures to protect themselves. One way to do this is to install anti-malware software on mobile devices and enable VPN functionality.
7. Protect your mobile phone password and voicemail pin. If your mobile phone does not currently have a password, add one that is at least six digits. Try to choose a unique password that is not already used across other systems and accounts. Do not use repeating digits in passwords or voice mail pins. Remember that your provider will never request your voice mail pin, so do not be tempted to provide it to anyone who requests it.

If you detect infection on an employer-issued device, immediately report your concern to the employee help desk or IT security staff personnel.

ARTICLE—ICSA LABS CONT...

“Mobile malware will continue to rise with increased smartphone use,” Hayter said, “but by following these tips users can help protect themselves and their personal data from unwanted intrusions.”

About ICSA Labs

ICSA Labs, an independent division of Verizon, offers third-party testing and certification of security products and network-connected devices, such as printers and faxes, to measure product compliance, reliability and performance to many of the world’s top security vendors. Visit <http://www.icsalabs.com> and <http://www.icsalabs.com/blogs> for more information.

Media contacts:

Brianna Carroll Boyle
703-859-4251
brianna.boyle@verizon.com

About Verizon

Verizon Communications Inc. (NYSE, NASDAQ:VZ), headquartered in New York, is a global leader in delivering broadband and other wireless and wireline communications services to consumer, business, government and wholesale customers. Verizon Wireless operates America’s most reliable wireless network, with more than 106 million total connections nationwide. Verizon also provides converged communications, information and entertainment services over America’s most advanced fiber-optic network, and delivers integrated business solutions to customers in more than 150 countries, including all of the Fortune 500. A Dow 30 company, Verizon employs a diverse workforce of nearly 196,000 and last year generated consolidated revenues of \$106.6 billion. For more information, visit www.verizon.com.

ARTICLE—WHO

WORLD UNITES TO HALT DEATH AND INJURY ON ROADS

Decade of Action for Road Safety 2011-2020 set to save millions of lives

6 May 2011 | Geneva - On 11 May, dozens of countries around the world kick off the first global Decade of Action for Road Safety 2011-2020. From New Zealand to Mexico and the Russian Federation to South Africa, governments are committing to take new steps to save lives on their roads. The Decade seeks to prevent road traffic deaths and injuries which experts project will take the lives of 1.9 million people annually by 2020.

To mark the launch of the Decade, governments in countries such as Australia, Cambodia, Ethiopia, Indonesia, Kuwait, Malaysia, Mexico, Niger, Nigeria, the Philippines, Slovenia, Sri Lanka, Uzbekistan and Viet Nam will host high-profile events and release national plans to improve safety and services for victims. A number of landmark national monuments will be illuminated with the road safety “tag”, the new symbol for the Decade. These include Times Square in New York City; Christ the Redeemer statue in Rio de Janeiro; Trafalgar Square in London; and the Jet d’Eau in Geneva, among others.

Curbing a growing health and development problem

“Today countries and communities are taking action vital to saving lives on our streets and highways” said WHO Director-General Dr Margaret Chan. “Road traffic crashes are a growing health and development concern affecting all nations, and the Decade offers a framework for an intensified response.”

ARTICLE— WHO CONT...

Road traffic injuries have become the leading killer of young people aged 15–29 years. Almost 1.3 million people die each year on the world's roads, making this the ninth leading cause of death globally. In addition to these deaths, road crashes cause between 20 million and 50 million non-fatal injuries every year. In many countries, emergency care and other support services for road traffic victims are inadequate. These avoidable injuries overload already stretched health services.

Global plan to improve the safety of roads and vehicles

"None of us should have to bear the grief and devastation caused by a road traffic crash" said Dr Etienne Krug, WHO Director of the Department of Violence and Injury Prevention and Disability. "The steps outlined in the Global Plan for the Decade are immediately doable, and will do much to spare the suffering of so many."

The Global Plan outlines steps towards improving the safety of roads and vehicles; enhancing emergency services; and building up road safety management generally. It also calls for increased legislation and enforcement on using helmets, seat-belts and child restraints and avoiding drinking and driving and speeding. Today only 15% of countries have comprehensive laws which address all of these factors.

Pedestrians, cyclists, and motorcyclists collectively represent almost half of those killed on the world's roads. Most of the progress has been made in the last few decades has been towards protecting people in cars. The Global Plan suggests measures that may afford these vulnerable groups protection – such as building cycle and foot-paths and separate motorcycle lanes or improving access to safe public transport.

If successfully implemented, the Global Plan's activities could save 5 million lives and prevent 50 million serious injuries over the course of the Decade. The Decade also aims at attracting donor funding to this issue. New York City Mayor Michael Bloomberg has already committed US\$ 125 million to support road safety in low-income and middle-income countries, by far the largest single donation to road safety. But other innovative funding mechanisms are being sought. For example, a voluntary "opt-out" scheme within the automotive sectors, in which US\$ 2 per new vehicle sold would go into a fund to support road safety in developing nations could raise at least US\$ 140 million a year.

WHO's role in the Decade of Action for Road Safety

WHO will play a role in coordinating global efforts over the Decade and will monitor progress towards achieving the objectives of the Decade at the national and international levels. WHO will also continue to provide technical support to national road safety initiatives aimed at decreasing drinking and driving and speeding; increasing the use of helmets, seat-belts and child restraints; and improving emergency care.

For more information, please contact:

Laura Sminkey

Communications officer, Department of Violence and Injury Prevention and Disability

WHO

Telephone: + 41 22 791 4547

Mobile: + 41 79 249 3520

E-mail: sminkeyl@who.int

http://www.who.int/roadsafety/decade_of_action/en/index.html

<http://www.decadeofaction.org>