

JUNE 2010

SOUTH AFRICAN INSURANCE CRIME BUREAU

ISSUE 6 : 2010

LISTS UPDATE:

Dräger

Hits : 204
Records: 1062
Number of lists: 14

SAPS 13

Hits: 17
Records: 180
Numbers of lists: 6

Tracker

Hits: 55
Records: 240
Number of lists: 12

DATADOT

Hits: 234 Data Dot and 21 other hits
Records: 234
Number of list: 5

Enquiries

Enquiries: 50
Replies: 183

**APPROX, R7,5 MILLION
SAVED BY INDUSTRY
TO DATE**

INSIDE THIS ISSUE...

SAICB UPDATE	1
LISTS UPDATE	1
FRAUDLINE	1
ARTICLE— 2010 REPORT TO THE NATIONS	3
ARTICLE— NEWORDER	7
ARTICLE—IT WEB SUMMIT 2010	8
CONTACT	9

SAICB UPDATE

SAICB UPDATE

It has been a busy month for the SAICB, with the training sessions for the Special Points of Contact (SPOC) beginning on 3 June, and the Fraudline and Staff dishonesty database initiatives being rolled out to the industry. In addition, the SAICB has seen further successes in it's cases and lists as well as positive responses from our training of the Lesotho Mounted Police Service (LMPS) and the South African Police Service (SAPS) border police.

SPOC Training

On 3 June 2010, the first training session was held for our SPOC's at the Summit Insurance Administration Services (SIAS) office in Centurion. The training was conducted by Lieutenant Colonel Bruce Davenport, from Priority Crime Investigation, Commercial Crime of the South African Police Service (SAPS).

The training was attended by representatives from: Standard Bank; Lion of Africa; Hollard; Absa; Santam; Legalwise; Telesure; SIAS and FRSTIA. The purpose of the training was to explain and provide refresher information on the following aspects:

- Purpose of a statement
- Contents of a statement
- Layout, structure and format of a statement according to legislation
- The difference between a statement and an affidavit
- The difference between and a declaration of a statement
- Whether 'hearsay evidence' is allowed in a statement
- The usage of abbreviations and Insurance lingo
- The description of an annexure in a statement and the marking of the annexure
- The value of a Comprehensive statement

Points that need to be addressed in the statements:

- Explain process of how conversations/scanned documents are attached to the

FRAUDLINE

In May 2010, **132** reports were received of which 13 reports were for the short term insurance industry, 1 report was received for Brokers and 2 reports for the life industry.

Since 2002, **26410** reports have been received of which **847** reports were for the short term industry **126** reports for the brokers and **335** 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

SAICB UPDATE CONT...

system/policy (electronic format)

- Who has access to recordings
- Whether alterations can be made to recordings

During the training session other aspects were also discussed for possible future training:

- Interviewing of clients by assessors – recordings
- Training for assessors/investigators on interviewing and notes on clients looks/way of speaking etc.
- Legislation regarding 'best evidence rule' – scanned documents/ copies/photos
- Statements of two people that are exactly the same are not allowed.

The training was well received by those attending the training session and further training sessions will be arranged in future—dates to be sent out once the planning is finalised. A special thanks to Lieutenant Colonel Bruce Davenport for giving us his valuable time and expertise on the day and SIAS for hosting the session.

Fraudline and Staff Dishonesty Database rollout

The Fraudline and staff dishonesty database initiatives are being rolled out to the member companies currently and is allowing the SAICB to reintroduce itself to the industry as well as the benefits of the Fraudline to members, and addressing any queries or questions the members may have about the Staff dishonesty database. A final report will be sent to the industry once all member companies have been covered. The feature article in this months Newsletter—from page 3—shows the importance of both these initiatives to the industry.

General

June has also been a very successful month from our cases and initiatives perspective, with the SAICB being instrumental in identifying and closing down a hoola hoop scam in one of our member companies, resulting in the arrest of the principal fraudsters and with a potential recovery of approximately R500 000 for the member company. One of the SAICB cases was presented in court on 18 June 2010 resulting in the accused pleading guilty and offering to pay back the monies defrauded from the industry. Sentencing has been postponed to 30 June 2010 where the details will be finalised. Five member companies were involved in this case. Approximate recovery for the members is R350 000.

The cloned vehicles initiative is already producing results with valuable contributions from the member companies regarding written off vehicles being instrumental in helping the SAICB identify the cloned vehicles on our roads and being insured by our member companies.

The cross border training and relationship building with our neighbouring countries has also produced results with the first identification of our member company vehicles in the Lesotho pounds to the value of approximately R127 000 and in Zimbabwe pounds to the value of approximately R170 000.

The first pound list from KwaZulu Natal (KZN) - Isipingo pound—has been received and sent to the industry for action, the first Dräger list from KZN has also been received and sent out to the industry.

The SAICB is in the process of finalising our relationships with the various tracking companies to receive their lists of stolen / recovered vehicles and property. We will report in the next Newsletter on which tracking companies have come on board. 📞

MEMBERS

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

PARTNERS

SOUTH AFRICAN
 INSURANCE
 ASSOCIATION (SAIA)
 TRANSUNION
 DELOITTE
 MEMEX
 SAFPS
 UNICODE
 BACSA
 NEWORDER
 DATADOT
 CGC
 TRACKER
 SABRIC

ARTICLE—2010 REPORT TO THE NATIONS

THIS REPORT IS OF PARTICULAR INTEREST TO THE SAICB AND ITS MEMBER COMPANIES BECAUSE OF THE TWO INITIATIVES THAT ARE CURRENTLY BEING ROLLED OUT TO THE INDUSTRY—NAMESLY THE INSURANCE FRAUDLINE INITIATIVE—INDUSTRY TIP-OFF LINE AND THE STAFF DISHONESTY DATABASE.

OCCUPATIONAL FRAUD COSTS \$2.9 TRILLION GLOBALLY

The Association of Certified Fraud Examiner's (ACFE) *2010 Report to the Nations on Occupational Fraud and Abuse* is based on data compiled from a study of 1,843 cases of occupational fraud that occurred worldwide between January 2008 and December 2009. All information was provided by the Certified Fraud Examiners (CFEs) who investigated those cases. The fraud cases in their study came from 106 nations including Africa — with more than 40% of cases occurring in countries outside the United States.

This expansion allows the ACFE to more fully explore the truly global nature of occupational fraud and provides an enhanced view into the severity and impact of these crimes. Additionally, the ACFE are able to compare the anti-fraud measures taken by organizations worldwide in order to give fraud fighters everywhere the most applicable and useful information to help them in their fraud prevention and detection efforts.

Key Findings and Highlights of the *2010 Report to the Nations* include:

The Impact of Occupational Fraud

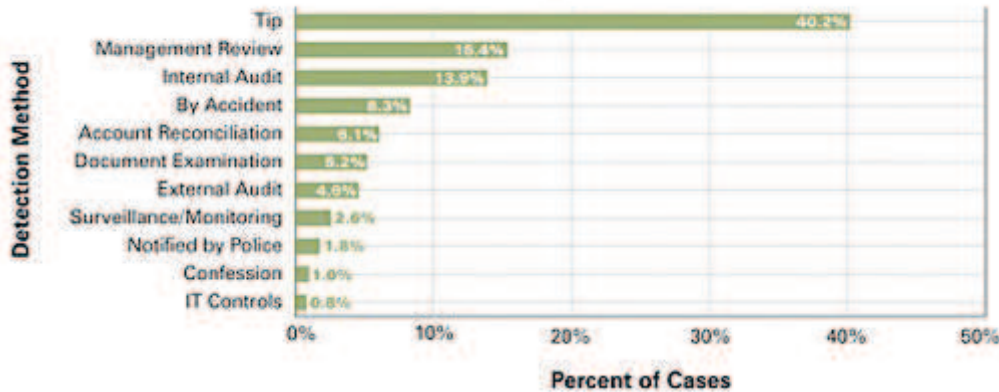
- Survey participants estimated that the typical organization loses 5% of its annual revenue to fraud. Applied to the estimated 2009 Gross World Product, this figure translates to a potential global fraud loss of more than \$2.9 trillion.
- The median loss caused by the occupational fraud cases in the study was \$160,000.
- Nearly one-quarter of the frauds involved losses of at least \$1 million.
- Small organizations are disproportionately victimized by occupational fraud. These organizations are typically lacking in anti-fraud controls compared to their larger counterparts, which makes them particularly vulnerable to fraud.

Fraud Detection

- The frauds lasted a median of 18 months before being detected.
- **Occupational frauds are much more likely to be detected by a tip than by any other means. This finding has been consistent since 2002 when the ACFE began tracking data on fraud detection methods.**
- Anti-fraud controls appear to help reduce the cost and duration of occupational fraud schemes. The ACFE looked at the effect of 15 common controls on the median loss and duration of the frauds. Victim organizations that had these controls in place had significantly lower losses and time-to-detection than those organizations without the controls.

ARTICLE—2010 REPORT TO THE NATIONS *CONT...*

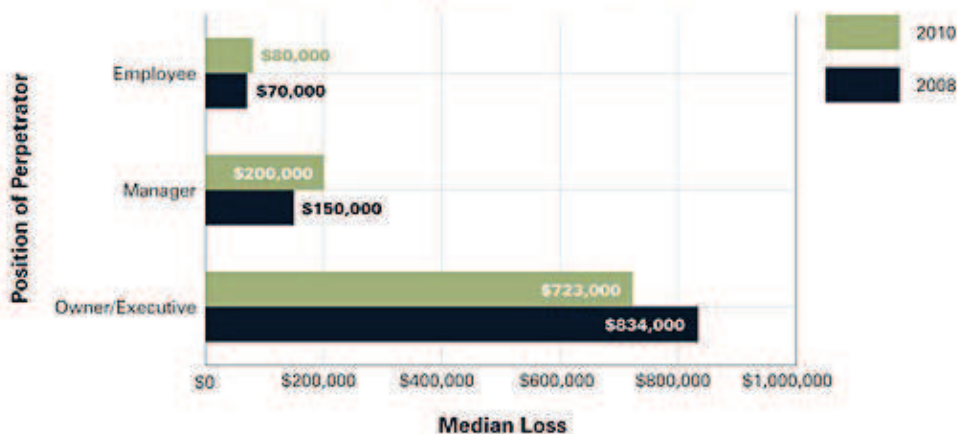
Initial Detection of Occupational Frauds



Perpetrators of Fraud

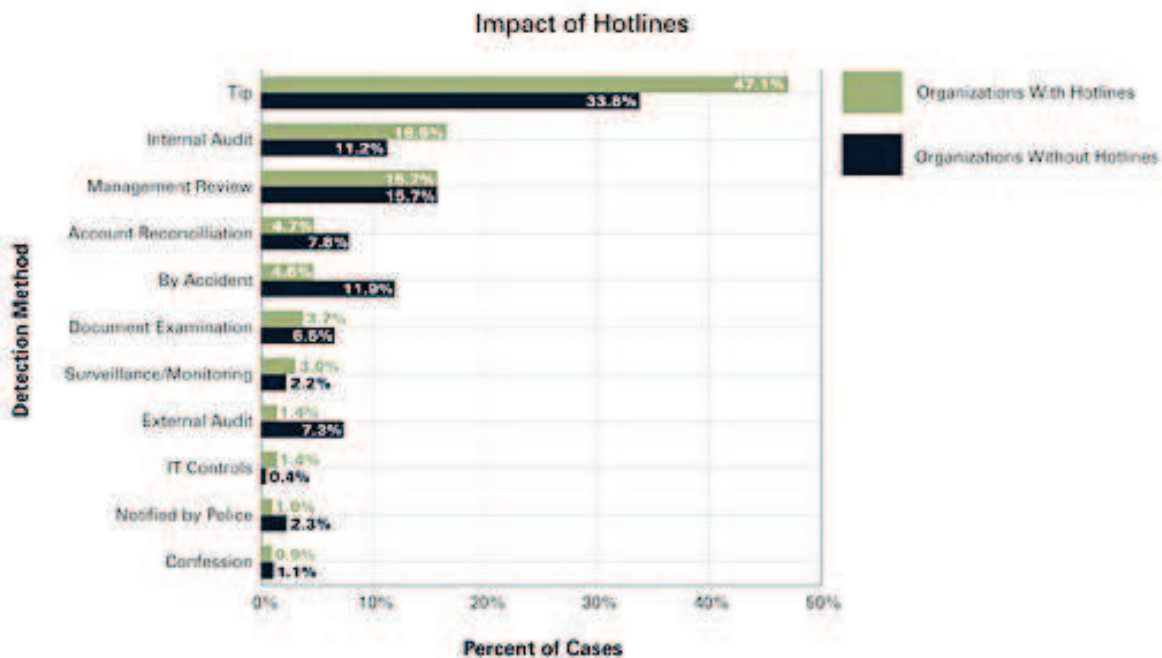
- High-level perpetrators cause the greatest damage to their organizations. Frauds committed by owners/executives were more than three times as costly as frauds committed by managers, and more than nine times as costly as employee frauds. Executive-level frauds also took much longer to detect.
- More than 80% of the frauds in the study were committed by individuals in one of six departments: accounting, operations, sales, executive/upper management, customer service or purchasing.
- More than 85% of fraudsters in the study had never been previously charged or convicted for a fraud-related offense. This finding is consistent with prior studies.
- Fraud perpetrators often display warning signs that they are engaging in illicit activity. The most common behavioral red flags displayed by the perpetrators in the study were living beyond their means (43% of cases) and experiencing financial difficulties (36% of cases).

Position of Perpetrator — Median Loss



ARTICLE—2010 REPORT TO THE NATIONS *CONT...*

- Occupational fraud is a global problem. Though some of the ACFE findings differ slightly from region to region, most of the trends in fraud schemes, perpetrator characteristics and anti-fraud controls are similar regardless of where the fraud occurred.
- Fraud reporting mechanisms are a critical component of an effective fraud prevention and detection system. Organizations should implement hotlines to receive tips from both internal and external sources. Such reporting mechanisms should allow anonymity and confidentiality, and employees should be encouraged to report suspicious activity without fear of reprisal.**



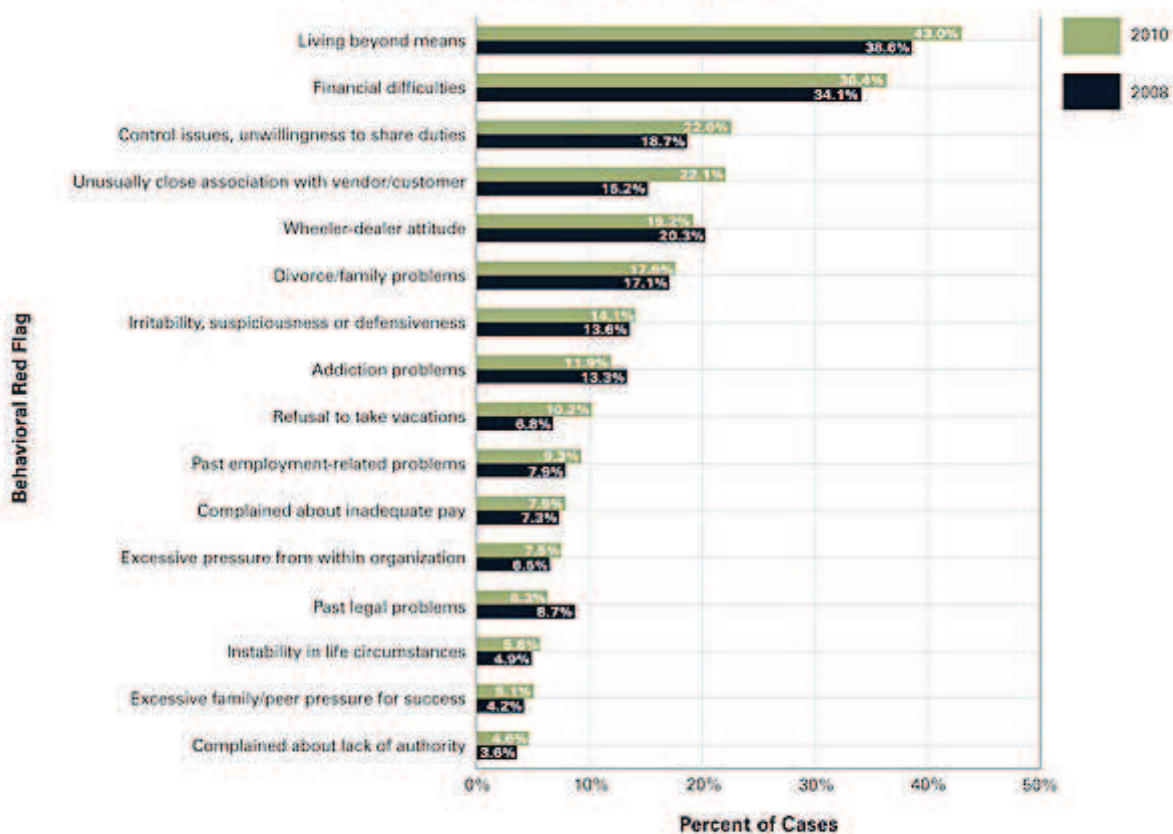
- Organizations tend to over-rely on audits. External audits were the control mechanism most widely used by the victims in our survey, but they ranked comparatively poorly in both detecting fraud and limiting losses due to fraud. Audits are clearly important and can have a strong preventative effect on fraudulent behavior, but they should not be relied upon exclusively for fraud detection.
- Employee education is the foundation of preventing and detecting occupational fraud. Staff members are an organization's top fraud detection method; employees must be trained in what constitutes fraud, how it hurts everyone in the company and how to report any questionable activity. Our data shows not only that most frauds are detected by tips, but also that organizations that have anti-fraud training for employees and managers experience lower fraud losses.**
- Surprise audits are an effective, yet underutilized, tool in the fight against fraud. Less than 30% of victim organizations in our study conducted surprise audits; however, those organizations tended to have lower fraud losses and to detect frauds more quickly. While surprise audits can be useful in detecting fraud, their most important benefit is in preventing fraud by creating a perception of detection. Generally speaking, occupational fraud perpetrators only commit fraud if they believe they

ARTICLE—2010 REPORT TO THE NATIONS *CONT...*

will not be caught. The threat of surprise audits increases employees' perception that fraud will be detected and thus has a strong deterrent effect on potential fraudsters.

- Small businesses are particularly vulnerable to fraud. In general, these organizations have far fewer controls in place to protect their resources from fraud and abuse. Managers and owners of small businesses should focus their control investments on the most cost-effective mechanisms, such as hotlines and setting an ethical tone for their employees, as well as those most likely to help prevent and detect the specific fraud schemes that pose the greatest risks to their businesses.
- Internal controls alone are insufficient to fully prevent occupational fraud. Though it is important for organizations to have strategic and effective anti-fraud controls in place, internal controls will not prevent all fraud from occurring, nor will they detect most fraud once it begins.

Behavioral Red Flags of Perpetrators²⁰



²⁰The sum of percentages in this chart exceeds 100% because in many cases perpetrators displayed more than one behavioral red flag.

ARTICLE—2010 REPORT TO THE NATIONS CONT...

- Fraudsters exhibit behavioral warning signs of their misdeeds. These red flags — such as living beyond one’s means or exhibiting control issues — will not be identified by traditional controls. Auditors and employees alike should be trained to recognize the common behavioral signs that a fraud is occurring and encouraged not to ignore such red flags, as they might be the key to detecting or deterring a fraud.
- Given the high costs of occupational fraud, effective fraud prevention measures are critical. Organizations should implement a fraud prevention checklist in order to help eliminate fraud before it occurs. 📌

THE FULL REPORT WILL BE POSTED ON THE SAICB WEBSITE - www.saicb.co.za OR PLEASE CONTACT MELANIE PILLAY ON melaniep@saicb.co.za TO SEND THE REPORT TO YOU.

Source: Association of Certified Fraud Examiners (ACFE), 2010 Report to the Nations on Occupational Fraud and Abuse. Thank you to Scott Patterson, Media Relations Specialist; Association of Certified Fraud Examiners, for permission to use this summary in our Newsletter and to distribute the full report.

ARTICLE—NEWORDER

NEWORDER INDUSTRIES has been appointed as the SAICB’s Enterprise Risk Management, Storage and Virtualisation partner

NEWORDER INDUSTRIES (Pty) Limited was recently appointed by the South African Insurance Crime Bureau (SAICB) to ensure that the SAICB maintains a high level of security and control over their systems and data in order to minimize their exposure to possible IT related security threats.

NEWORDER INDUSTRIES is a local company that provides specialised enterprise risk management, IT security, virtualisation and storage solutions to corporates. Its services and solutions are designed to help corporates meet their growing IT infrastructure needs in the most cost-efficient way, and address enterprise risk management holistically to ensure good governance and compliance with King-III.

What does this mean? NEWORDER INDUSTRIES will provide expert consulting to the SAICB on enterprise risk management, IT security and governance. It will also deliver the appropriate, industry leading technologies in support of this. As a specialist third party, NEWORDER INDUSTRIES has an objective approach to evaluating the organisation, its people and its systems in an unbiased way.

NEWORDER INDUSTRIES managing director, Marthinus Engelbrecht says: “The SAICB, like all companies, faces enormous challenges when it comes to managing IT-related security risks in light of escalating IT fraud, increasingly sophisticated attack methods, new legislation around the archiving of electronic communication and transactions, and compliance with King-III.

NEWORDER INDUSTRIES is part of the Orcom Group, which is a level 3 BEEE contributor. 📌

Thank you to Mia van Heerden and Marthinus Engelbrecht for the article, for further information on NEWORDER INDUSTRIES, please contact Marthinus on marthinus@neworder-ind.net

ARTICLE—IT WEB SUMMIT 2010

IT WEB SUMMIT 2010

The one thing I came away with from the IT Web Summit 2010 is that we are, on the whole, ill prepared and/or unaware of the threat against us as an industry as well as individuals when it comes to IT security and risks. With the growing plethora of malware (Trojans, viruses, worms, spyware, botnets, spam and phishing) and social engineering rapidly climbing the ranks in terms of ease of use and prevalence, it is time for people to realise that our computer systems are under constant threat.

Firstly, lets define some of these terms with examples of where they might occur in and around our industry:

Malware

Short for "malicious software," malware refers to software programs designed to damage or do other unwanted actions on a computer system.

Virus

Computer viruses are small programs or scripts that can negatively affect the health of your computer. These malicious little programs can create files, move files, erase files, consume your computer's memory, and cause your computer not to function correctly. Some viruses can duplicate themselves, attach themselves to programs, and travel across networks. In fact opening an infected e-mail attachment is the most common way to get a virus.

Trojan

Trojans are software programs that masquerade as regular programs, such as games, disk utilities, and even antivirus programs. But if they are run, these programs can do malicious things to your computer. Unlike viruses, however, Trojans don't replicate themselves, though it is possible for a Trojan to be attached to a virus file that spreads to multiple computers.

Worm

A computer worm is a type of virus that replicates itself, but does not alter any files on your machine. However, worms can still cause havoc by multiplying so many times that they take up your entire computer's available memory or hard disk space. Although worms initially started life merely proving that programmers could compromise numerous PC's in as short a time as possible, they can nowadays deliver viruses and other destructive payloads.

Spyware

As the name implies, this is software that "spies" on your computer. Nobody likes to be spied on, and your computer doesn't like it either. Spyware can capture information like Web browsing habits, e-mail messages, usernames and passwords, and credit card information. If left unchecked, the software can transmit this data to another person's computer over the Internet. These are not only key loggers but include screen capture programs. Hardware (physical equipment on your PC) also has the ability to capture your information.

Botnet

The word BOTNET is short for the combination of the word **robot** and **network**. The term often applies to groups of computer systems that have had malicious software installed by worms, Trojans or other malicious software that allows the "botnet herder" or botnet's originator to control the group remotely. These botnets are then either sold or used to harvest information or attack other networks.

Spam

Unsolicited e-mail normally sent in bulk. This is also a favourite means for distributing viruses and potentially harmful payloads. A compromised PC is often used to propagate viruses by targeting all or some of the contacts on said PC.

ARTICLE—IT WEB SUMMIT 2010 *CONT.....*

Phishing

Phishing is a con game that scammers use to collect personal information from unsuspecting users. The false e-mails often look surprisingly legitimate and even the Web pages where you are asked to enter your information may look real.

Social Engineering

While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

So what can we do?

It looks like an impossible task but by applying a few easy to use solutions and practices, one can prevent the majority of attacks.

The first and probably most essential fix is to install decent anti-virus software. A lot of research has been put into and is still going into anti-virus software on a daily basis. There is a lot of information available regarding the effectiveness of the products on offer, so a bit of research is necessary when choosing the right product. Because of the changing nature of malware it is essential that your anti-virus definitions are up to date.

As a general rule, don't open a program unless you know it is legitimate. This applies especially to e-mail attachments that are executable files. Even if you are pretty sure the attachment is OK, it is still a good idea to run it through your virus scan program (with the latest virus definitions) just to be safe.

Apply patches and updates regularly. This does not only apply to your anti-virus program. Software vendors are continually improving their products and "fixing" holes or security flaws. As a rule these updates are free or part of the licensing cost and on certain products require manual intervention.

Another general rule which has been taught since we were children is not to give personal information to un-trusted/unknown persons. With the increase in social networking, e-commerce and the use of the internet in general, there has been a parallel, if not exponential, growth in social engineering and phishing type attacks. Too easily people hand private information, from family or address detail to account and PIN detail, over to the faceless internet. Things to watch out for include ensuring that the websites visited are secure when supplying personal information, that the site is actually who it claims to be and , in

the case of social networking sites, your information is shared on an acceptable level for your risk requirements.

In big organisations large amounts of money are spent securing their assets by buying the latest, strongest antivirus and firewall software and many other forms of protection. However, the target of these attacks in most cases is not being addressed – the individual. No matter the security employed, if the person at the PC is not educated in the risks then they will effectively be opening the door for the attackers. Just as people are taught about the dangers of crossing the street, so they should be educated on the risks involved in using the internet. 📧

Sources

<http://www.techterms.com/>
<http://www.michigan.gov/cybersecurity/>
<http://en.wikipedia.org/>

THANK YOU TO MARC NICHOLSON FOR THIS ARTICLE AFTER HE ATTENDED THE IT WEB SUMMIT IN MAY 2010.

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