

SEPTEMBER 2009

SOUTH AFRICAN INSURANCE CRIME BUREAU

ISSUE 7 : 2009

IN BRIEF....

EVENTS OF INTEREST

- Opening of the new Alcohol Testing Center in Randburg which took place on 29 September 2009. This is the second center in Gauteng, and a third will be opened in Soweto, by the end of the year.
- SAICB "Year in Review" breakfast which is scheduled for 4 November 2009, to update the industry, public and interested parties on what has been achieved in the year under review and the way forward for the SAICB.

INSIDE THIS ISSUE...

SAICB UPDATE	1
FRAUDLINE	1
ARTICLE—ITWEB	2
INFORMATION SHARING UPDATE	2
ARTICLE—CSFS	3
ARTICLE—ACFE	6

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

SAICB UPDATE

With the SAICB budget for 2009/2010 approved, the invoicing was sent out in early September for the fixed portion of the fees. It was decided that the budget would be split 50/50— with 50% being a fixed amount and the other 50% based on the market share of the member company. The market share invoice portion of the budget will be sent out before end October .

The Fraudline funding, while compulsory for members, was also opened to the industry for funding and three additional companies have agreed to assist with this industry initiative, with a fourth still pending. The Fraudline invoicing has also been sent out.

The scheduled review workshop took place on 30 September 2009, with Vivienne Pearson from the South African Insurance Association (SAIA) acting as facilitator. The workshop was extremely successful in reviewing what has been achieved in a very busy and successful first year, while providing set objectives and direction for the next year. Thank you to all who participated in the workshop.

An executive summary that reviews the past year and provides direction for the new year has been drafted , and will be sent to the industry shortly, and with the October invoicing for member companies. The SAICB will be hosting a "Year in Review" breakfast on 4 November 2009 in Johannesburg to update the industry, media, stakeholders and partners on the previous years achievements, and the way forward. Invitations for this event will be send out in early October.

The current cases being investigated by the SAICB have progressed significantly, and the SAICB has began with the analysis and investigations of the results from the business rules. This is a very detailed and lengthy process and progress will be reported in future issues.

The Board has decided refocus the SAICB's activities to concentrate specifically on the results of the business rules and current cases. Enquiries will still be processed, but details of the process will be sent to the members shortly. The lists received from the South African Police Services (SAPS) - SAPS 13 lists, the Johannesburg Metropolitan Police Department

FRAUDLINE

In August 2009, **123** reports were received of which 5 reports were for the short term insurance industry, 1 report on brokers and 2 report for the life industry.

Since 2002, **25301** reports have been received of which

764 reports were for the short term industry **120** reports for the brokers and **318** reports were for the life industry.

For the full report with all the statistics, please contact Melanie Pillay on melaniep@saicb.co.za

(JMPD) - Dräger lists - and the National Prosecuting Authority (NPA) Assets Forfeiture Unit, will still be processed and sent to the industry for information and action.



0860 002526
insurance@fraudline.co.za

SEPTEMBER 2009

SOUTH AFRICAN INSURANCE CRIME BUREAU

ISSUE 7 : 2009

MEMBERS

SANTAM
 MUTUAL & FEDERAL
 HOLLARD
 ZURICH
 LION OF AFRICA
 REGENT
 TELESURE
 ABSA INSURANCE
 STANDARD BANK
 INSURANCE
 FRSTIA (SIAS,
 OUTSURANCE, MO-
 MENTUM)
 MIWAY

PARTNERS

SOUTH AFRICAN
 INSURANCE
 ASSOCIATION (SAIA)
 TRANSUNION
 FRAUDLINE
 MEMEX
 SAFPS
 UNICODE
 BACSA
 CSFS

ARTICLE—ItWeb

RECESSION SEES DATA WALK OUT THE DOOR

Almost 40% of South Africans take corporate information with them when they move jobs, according to a survey conducted by Symantec and Moneyweb.


Gordon Love, regional director for Africa at Symantec, believes organisations face a greater risk of data loss because of the difficult economic conditions.

Love says the level of awareness around this kind of theft is relatively low, which creates a challenge for companies in policing the actions of employees when they leave the organisation.

“In many situations, the employees concerned are not aware that they are taking confidential information and, in essence, stealing from their employer. In other situations feelings of resentment towards a former employer may spur them on to take as much information as possible.

“It is critical that not only are employees properly educated about what they can and can't take with them when they leave, but also that those employees that are leaving are properly screened to keep the theft of intellectual information to a minimum.”

The survey revealed that human resources practitioners are not sufficiently equipped when it comes to data security issues, and even when an exit interview is performed, the employee is not quizzed on what documents they are taking with them.

According to Symantec, the results of the South African survey are better than those from a similar survey conducted in the US earlier this year. In the US survey, 59% of employees admitted to taking data from former employers, many of whom stole data intentionally to secure future employment. 

This article appeared in the ItWeb website on 28 August 2009 - www.itweb.co.za


INFORMATION SHARING UPDATE—SEPT 2009

12 general and Fraudline enquiries were received and sent to the industry, with 22 responses received from the industry to the enquiries.

13 SAPS 13 and Specialised Investigative Unit (SIU) lists were received with 3934 records that resulted in 98 hits on Memex to date, this is still ongoing .

13 Tracker lists were received with 214 records that resulted in 76 hits in Memex.

8 Dräger lists were received with 369 records that resulted in 112 hits in Memex.

Information sharing has resulted in approximately R1,51 million savings for the industry since June 2009. 

ARTICLE—CSFS

COMPUTER SECURITY & FORENSIC SOLUTIONS (CSFS)

Who we are and what we do:

Computer Security & Forensic Solutions; (better known as CSFS) within the South African and Africa Regions, was founded in 1999. Our primary focus is to deliver Cyber, Computer and Network IT Forensics, IT Security services and solutions, IT Risk assessments and IT Business Intelligence services equal to best International standards.

The uniqueness of CSFS is embedded in the diversity of experience and knowledge brought together in a motivated team of investigation and security experts, with distinguished careers in IT Forensics, IT Security, IT Intelligence and IT Governance. Combining all our expertise and skills, we are able to provide a sound forensic service to corporate entities.

CSFS was bound together to provide a global IT Security and IT Forensic solution, because any company is equally vulnerable from the inside as well as the outside. The focus of CSFS is to provide in-house custom developed solutions, with the ability to MANAGE THE RISK, in a manner which will not only provide the client with greater security on their network and the Internet, but also enable them to institute prosecution in whatever form. The client will have peace of mind knowing that;

- Network environments are protected;
- Information management is intact;
- External and internal risks are profiled;
- IT Forensics is in place;
- IT Security is proactive and preventative and
- IT experts are on standby in a case of emergency.

For more information visit: www.csfs.co.za or e-mail marthinus@csfs.co.za to arrange for a more in-depth and technical presentation.

Cyber Crime is on the rise and it can happen to anyone!

If you think this has nothing to do with you, you are WRONG. These types of crimes impact you personally and your company and can happen to anybody. Your personal or company information can be stolen, and once in the wrong hands your information can be used to obtain and purchase illegal credit and bank cards, illegal identity documents and perform illegal financial transactions leaving you liable for all losses and possible facing criminal charges.

Whilst most personal and company financial transactions are nowadays performed over the Internet makes the Internet the largest target for criminal activities by Hackers and cyber criminals. Statistics indicates that the financial systems within corporate organizations are mostly targeted, and to be misused to perform fraudulent transactions. An estimate of 80% of such criminal activities is initiated from within an organizations network environment, by lack of; the proper IT Se-

ARTICLE—CSFS *cont.....*

curity / IT Forensic and IT Intelligence solutions and measures not being implemented, IT Security not being maintained and miss management of the corporate network environment.

Syndicates have identified this and have already established themselves in South Africa, and a huge increase in Cyber Crimes activities could be expected up to the 2010 Soccer World Cup and beyond. Since November 2008 to date, CSFS have investigated more than thirty different cases of cyber crimes involving more than 2 Billion rand.

Syndicates and cyber criminals are willing to invest huge amounts of money at a time, to later on gain millions. Once cyber criminals have the username and password of the financial system they could manipulate and transfer money from your personal or company accounts. They can perform these actions from anywhere, even while on holiday in other Countries.

Corporate entities lose millions of rands at a time and without any log files or audit trail available, which was destroyed during the attack, resulting in no hope to recover any financial losses.

Corporate entities should invest in reputable and trusted companies to conduct comprehensive vulnerability and risk assessments to determine the current risk and to address those risks.

During Cyber Crime Investigations, it was identified that:

Company networks are vulnerable; Syndicates compromised company employees; Unauthorized company employees have access to Management and financial system; Authorized company employees / IT managers has access to financial passwords and usernames; The unlawful interception of passwords and usernames by hackers and cyber criminals; The installation of malicious software (spyware) on network systems by cyber criminals and company employees; Company financial and Management systems are not properly secured; Companies contracted IT Forensic companies which is not capable to conduct such investigations; The unlawful interception of board meeting notes and company information which was distributed as e-mail attachments and Company data manipulation.

We also identified the following Network defects:

- Network infrastructure that is not correct designed and implemented;
- No Management information;
- Network security insufficiency;
- No real-time monitoring of communication flow;
- Lack of remote access security;
- Lack of periodic network assessments/auditing;
- No perimeter defense solutions in place and
- No business intelligence information available.

Business intelligence information can be defined as; to be in a position at any given time to have insight information on

ARTICLE—CSFS *cont...*

communication, inside the network, against the network and leaving the network.

During the past ten years CSFS investigated over 5000 cyber and computer crimes and have identified that hackers, cyber criminals and syndicates have made use of the under mentioned methods to defraud Corporate entities and gained access to networks and computers:

- Hacking;
- Social Engineering;
- Phishing and spam attacks;
- Malicious attacks;
- Target massaging attacks;
- Web browsing attacks;
- Network attacks;
- Malware / Spyware attacks and

Botnet attacks. A "botnet" is a network of zombie computers, thousands of computers, up to millions of computers are indirectly infected with malicious code that allows an unauthorized user to control them via the Internet, without the knowledge of the owner of the computer. The computers are used to spread: Spam; Viruses; DOS (Denial-of-service) attacks and hacking to conduct fraudulent and other activities.

How can businesses protect themselves against these and other attacks? CSFS has developed in-house custom solutions which have been successfully implemented inside corporate entities to protect:

- External communication flow;
- Internal communication flow;
- Server environment;
- User environment and
- Insecure environment.

These solutions are linked with a 24/7/365 real-time forensic network monitor solution with secure operation centre (SOC) functionality.

CSFS has also developed a secure mail solution to prevent unauthorized interception of confidential business, board meeting notes and company information.

Final Note: With regards to your personal banking information: Do not divulge your personal information by clicking on a link you received via e-mail. Verify that you enter your details on the correct website and verify all security measures on the site. Your bank will NEVER ask you to verify or divulge your personal information by sending you an e-mail. Such verifications should ONLY be done at your local bank branch.

ARTICLE—ACFE

WHEN THE ECONOMY TURNS DOWN, FRAUD TURNS UP!

(this article looks at occupational fraud)

Intense financial pressures during the current economic crisis have led to an increase in fraud, according to a survey of fraud experts conducted by the ACFE (Association of Certified Fraud Examiners). Results of the survey, published in the new ACFE report "Occupational Fraud: A Study of the Impact of an Economic Recession," also found that staff layoffs are pervasive and are leaving holes in organizations' internal control systems.

While it's not surprising that the majority of experts say the economic crunch has led to an increase in occupational fraud, what is amazing is that some companies are contributing to or even creating their current high fraud risk and are not doing enough to address this increased risk.

As Association of Certified Fraud Examiners (ACFE) president James Ratley says...

"While everybody could guess in hard economic times fraud was going to go up, what struck me as unusual about the findings was that, despite the number of respondents who say fraud has increased, most don't intend to spend more on fraud prevention, - to me, that's wishful thinking!"

Here are some of the key findings:

- More than half (**55.4%**) of respondents said that the **level of fraud has increased** (slightly or significantly) in the previous 12 months compared to the level of fraud they investigated or observed in years prior. In addition, 49% observed an increase in the dollar amount lost to fraud during the same period. We have seen increases in fraud in countries such as Botswana and Namibia, who traditionally had low levels of fraud and crime syndicate activity. Our predications are that fraud in Southern Africa will get far worse, especially with the 2010 Soccer World Cup that is estimated will attract about 500 000 visitors. Obviously criminals will be amongst these soccer fans as they know that they will have some nice opportunities to do their dirty deeds under cover of the excitement of the soccer fever.
- About half (**49.1%**) of respondents cited **increased financial pressure** as the biggest factor contributing to the increase in fraud, compared to increased opportunity (27.1 %) and increased rationalization (23.7%). These are the three elements making up the 'fraud triangle'.
- **Employees pose the greatest fraud threat** in the current economy. Many organisations, however, focus on the external threat (customers, vendors) and assume that their staff members are all honest. This is a big mistake as most fraud is perpetrated by 'trusted employees'. Please keep in mind that fraud is a crime of **deception** so if you do not trust someone they cannot defraud you can they?
- When asked which, if any, of several categories of fraud increased during the previous 12 months, the largest number of survey respondents (**48%**) indicated that **embezzlement was on the rise**. For those of you that don't know what the word embezzlement means here is the definition: **Theft of money, under that employee's control, from an employer by an employee using false entries in accounting records to cover up the crime. An embezzler is typically an accountant, bookkeeper or manager who is able to divert income and then cover it up.**
- Most frauds are detected only after 2 – 3 years of embezzlement so think how much money you could lose if you have

ARTICLE—ACFE *cont...*

an embezzler in your organisation! How will you know – well he or she won't put up their hand if you pose this question at the next staff meeting – you have to look for the symptoms of embezzlement using data analytical tools as an example, which will then lead you to the embezzler. It's like going to the doctor for an annual check-up and he tests your blood pressure, takes blood samples, listens to your heart-beat etc. In the same way you need to check your business for symptoms of fraud at least every year. Fraud, like cancer, does not want to be found but if you find it soon enough you can prevent it spreading.

- Additionally, **37%** say frauds by **unrelated third parties have increased** and roughly 20% indicate frauds by vendors, financial statement fraud, and corruption have increased.
- Layoffs are leaving holes in organizations' internal control systems. Nearly **60%** of CFEs who work as in-house fraud examiners reported that their companies had experienced layoffs during the past year. Among those who had experienced layoffs, almost **35%** said their company had **eliminated some controls**, while 44.2% said the layoffs had no effect on controls and only 3.2% said their company had increased controls. By retrenching employees segregation of duties, a critical internal control, is affected. If one person is responsible for numerous functions this hugely increases the risk of fraud occurring. And if some controls are totally eliminated then the organisation is looking for trouble – it's like a person who has not had a vehicle accident in the last year saying that they will now remove some of their air-bags and take out the ABS brakes in order to make the car lighter. All they have done is make themselves more vulnerable to injury should they have an accident - it's the difference of a minor or fatal accident.
- Fraud levels are expected to continue rising. Almost **90%** of respondents said they expect **fraud to continue to increase during the next 12 months**. Well of course fraud levels will rise – the victims are making sure of this by eliminating controls, laying off staff members, and not providing budget for an anti-fraud program. When the economy is down is when an organisation most needs proper fraud prevention procedures! In a high-risk fraud environment – which some organisations may have created inadvertently through layoffs and other cuts – they need to increase both their fraud prevention and their detection techniques. Of the two, James Ratley says, prevention is the bigger issue. ***"It's such an uncomfortable topic; people are hesitant to address it."***

The current recessionary economy will most probably be with us for the rest of 2009 and maybe even into 2010 so it's crucial that organisations start implementing fraud prevention programs or evaluating whether their existing fraud prevention program elements are working properly. Keep in mind that it's not a recession for criminals – they are more active now than ever!

"The message is simple: Desperate people do desperate things," said ACFE President James Ratley. ***"Loyal employees have bills to pay and families to feed. In a good economy, they would never think of committing fraud against their employers. But especially now, organizations must be vigilant during these turbulent times by ensuring proper fraud prevention procedures are in place."***

Source: ACFE

The full survey can be downloaded here:

<http://www.acfe.com/documents/occupational-fraud.pdf>

Thank you to Mario Fazekas, Certified Fraud Examiner (CFE) for permission to use this article that appeared in the 2009 Exactech Newsletter, Issue 2 2009.