

MARCH 2011

SOUTH AFRICAN INSURANCE CRIME BUREAU

ISSUE 02 : 2011

INFORMATION UPDATE:

From 26 Feb. 2011 to 29 Mar. 2011

Dräger

Number of lists: 4

Records: 921

Hits: 339

Tracker

Number of lists: 7

Records: 162

Hits: 50

SAP13

Number of lists: 31

Records: 566

Hits: 140

Enquiries

Enquiries: 60

Replies: 228

INSIDE THIS ISSUE...

SAICB UPDATE 1

FRAUDLINE 1

INFORMATION UPDATE 1

ARTICLE— KASPERSKY 2

ARTICLE— CIFAS 4

ARTICLE—SAICB VACANCY 8

CONTACT 9

SAICB UPDATE

SAICB UPDATE

The SAICB strategic session and first Board meeting has now taken place and the SAICB strategy for the next 5 years has been reviewed and approved. The SAICB will be increasing its staff complement and the first of the positions available appears in this newsletter on page 8.

The SAICB Communication Strategy has also been reviewed and approved with several components already being implemented. The strategy addresses relationship building on all levels and ensures that the general public is informed on our initiatives and mechanisms we have in place to report suspected fraud and crime, such as the Insurance Fraudline. More detailed programmes will begin in the new financial year.

Report back on the strategies will appear in future issues.

IN THIS ISSUE:

The article on page 2 on Cybercrime is a follow up to the article in last months issue on the impact of cybercrime over the past decade. This article deals with what is anticipated in the next decade. The issue of data security has become one of extreme significance in the financial industry and members and partners must ensure that they are aware of the threats in cyber-verse regarding their company's systems and particularly the threats to their data. The protection of your company's data must become part of your ongoing company strategy.

The article on page 4 deals with staff dishonesty and fraud and how to recognise the motivations and suspicious behaviour and what can be done to address it. The link between organised crime and staff involvement has been recognised as an integral part of the modus operandi of syndicates, and companies that are aware of this link can confront and hopefully prevent this threat by developing and putting in place systems and procedures to address this.

The SAICB has a staff vacancy for an Investigations Manager, the job description appearing on page 8. Please submit application by latest, Friday, 15 April 2011.

FRAUDLINE

In February 2011, **150** reports were received of which **10** reports were for the short term insurance industry, **1** report was received for Brokers and **2** reports for the life industry.

Since 2002, **27780** reports have been received of which **946** reports were for the short term industry **139** reports for the brokers and **380** 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

PARTNERS

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

ARTICLE— KASPERSKY

CYBERCRIME OUTLOOK 2020 March 2011

Kaspersky Lab presents its forecast for the IT threat landscape for the period 2011-2020. The forecast is based on an analysis of the main changes and issues in the sphere of IT security over the past decade, as well as emerging trends in the development of personal computers, mobile phones and operating systems.

According to the company's analysts, the most significant trends of the last 10 years (2001-2010) were:

** Mobility and miniaturisation. Smaller and smaller devices can now access the Internet from virtually any point on the globe; making wireless networks the most popular method of connecting to the Web.*

** The transformation of virus writing into cybercrime.*

** Windows maintaining its leading position as a vendor of operating systems for personal computers.*

** Intense competition in the mobile platform market with no clear-cut leader.*

** Social networks and search engines are the primary services of today's Internet.*

** Internet shopping – this sector already generates revenues that dwarf the annual budgets of some countries.*

The defining feature of the next decade will be the end of Windows' domination of user operating systems. Though Microsoft's brainchild will remain the primary business platform, everyday users will have access to an ever-expanding variety of alternative operating systems. Notably, even now the number of devices accessing the Internet via Windows and non-Windows platforms are almost the same, with the latter even occasionally exceeding their Microsoft counterparts.

The growing number of new operating systems will affect the process of threat creation - cybercriminals will not be able to create malicious code for large numbers of platforms. This leaves them with two options: either target multiple operating systems and have many individual devices under their control, or specialise in Windows-based attacks on corporations. The second variant will probably appeal to them more – by 2020, targeting individual users will become much more complex as the emerging trend of making payments electronically and using online banking will continue, however biometric user identification and payment protection systems will become the norm.

The coming changes in operating systems and their specifications will affect virus writing techniques as these new systems evolve. Many cybercriminals who used to target Windows devices will have to become adept at exploiting the new-generation operating systems. To retain their place in the sun, today's cybercriminal will need to enlist the help of members of the

ARTICLE— KASPERSKY CONT...

younger generation who are capable of writing malicious code for the new platforms. However, this state of the affairs cannot prevail forever and we may well see turf wars between different hackers and hacker groups.

Cybercrime in 2020 will almost assuredly divide into two groups. One group will specialise in attacks on businesses, sometimes to-order. Commercial espionage, database theft and corporate reputation-smearing attacks will be much in demand on the black market. Hackers and corporate IT specialists will confront each other on the virtual battlefield. State anti-cybercrime agencies will probably be involved in the process too and will have to deal predominantly with Windows platforms, in addition to the latest versions of traditional *nix systems.

The second group of cybercriminals will target those things that influence our everyday lives, such as transport systems and other services. Hacking such systems and stealing from them, making free use of them and the removal and changing of personal data about customers' activities will be the main focus of attention of the new generation of hackers, who will make a living this way.

The trend that has seen the Internet become both a popular resource for communication, entertainment and news, and a specially designed tool for Internet commerce and online payments, etc. will continue. The online user-base will expand to include many mobile and smart devices capable of using the Web to exchange or transfer information without the need for human intervention.

Botnets, one of today's most potent IT threats, will evolve dramatically. They will incorporate more mobile and Internet-enabled devices, and zombie computers as we know them will become a thing of the past.

The tools and technologies used in the field of communications will undergo massive change. These changes will see greatly increased data transfer rates and enhancements that will make the virtual communication experience much closer to that of real-life - by 2020, communication via the Internet with the help of a keyboard will be the stuff of old movies, meaning spammers will need to seek out new ways of delivering their unwanted correspondence to addressees across the globe. The first step the spammers will take is to change from targeting desktops to mobile devices. The volume of mobile spam will grow exponentially, while the cost of Internet-based communications will shrink due to the intensive development of cellular communication systems. As a result, users will be less likely to worry about unwanted advertising material.

The old adage knowledge is power will be more relevant than ever before. The struggle for the means to collect, manage, store and use information, about everything and everybody, will define the nature of threats for the next decade. Therefore the problem of privacy protection will be one of the key issues of the decade.

**THANK YOU TO KASPERSKY LAB. FOR PERMISSION TO USE THIS ARTICLE IN OUR NEWSLETTER.
FOR FURTHER INFORMATION PLEASE GO TO : www.kaspersky.com**

About Kaspersky Lab

Kaspersky Lab is the largest antivirus company in Europe. It delivers some of the world's most immediate protection against IT security threats, including viruses, spyware, crimeware, hackers, phishing, and spam. The company is ranked among the world's top four vendors of security solutions for endpoint users. Kaspersky Lab products provide superior detection rates and one of the industry's fastest outbreak response times for home users, SMBs, large enterprises and the mobile computing environment. Kaspersky® technology is also used worldwide inside the products and services of the industry's leading IT security solution providers. Learn more at www.kaspersky.com For the latest on antivirus, anti-spyware, anti-spam and other IT security issues and trends, visit www.securelist.com

ARTICLE—CIFAS

THE INTERNAL BETRAYAL

A CIFAS report on beating the growing threat of Staff Fraud

While attention has traditionally been focused upon external attempts to defraud, increasingly the fraud threat is being mirrored internally.

In 2009, CIFAS Staff Fraud Members noted a 45% increase in the number of cases of fraud committed by employees, compared with 2008. This included theft of cash from the organisation or a customer account, or lies on an application form, through to the theft or disclosure of commercial or personal data. The opportunities to commit fraud from the inside are numerous.

In *The Internal Betrayal*, CIFAS and a wide range of fraud prevention bodies and experts have combined to examine the facts about staff fraud. This report looks at the steps that organisations can take in order to combat the threat successfully.

From the recruitment process, expenses claims, whistle blowing and corruption, to ensuring that the right anti-fraud philosophy is present at all organisational levels, you will find in this report all that you need to know about combating the threat of staff fraud.

Peter Hurst
Chief Executive CIFAS – the UK's Fraud Prevention Service

CIFAS

CIFAS is a not-for-profit organisation, concerned solely with the prevention of fraud and is funded by subscription. For further details about any of the articles in this report, please contact CIFAS at memberservices@cifas.org.uk

Website: www.cifas.org.uk ; www.identityfraud.org.uk

Staff Fraudsters - the Link to Organised Crime CIFAS Reports

CIFAS Member organisations are facing an alarming rise in the volume of identity fraud. These frauds are being carried out by a number of different types of criminal; from the opportunist stealing the identity and good name of their friends and family, to the serious organised criminals indiscriminately tarnishing the financial reputation of anyone whose details they can find.

This rather begs the question; how are these criminals getting their hands on other people's identities? The finger of blame is pointed pretty squarely at the internet. The digital age has provided myriad different options for fraudsters of any level of expertise: from social engineering facilitated by social networking sites, to the deployment of complex malware designed to rip personal information from the hard drives of the defenceless.

It should be noted, however, that the finger of blame is not unwavering in its accusations as it is also wagging sternly at those staff fraudsters who disclose personal data to third parties. Yes, there are those who willingly disclose their employer's client information to those who would use it to commit further fraud – possibly against that same employer. It could be that these individuals have been approached by the criminals and offered money in exchange for personal and account information.

Another possibility is that these people have been specifically planted within the organisations with the express aim of farming off the data. The recorded number of these individuals is increasing. In 2008, there were 15 individuals recorded on the CIFAS Staff Fraud Database for unlawfully obtaining or disclosing personal data. This increased to 32 individuals in 2009,

ARTICLE—CIFAS CONT...

and the first half of 2010 has already seen a further 26. A straight line extrapolation would see the total for 2010 reach 52 – so, the recorded instances of this offence increased 113% in 2009 compared with 2008, and a further 62% increase is expected in 2010. It's true that the numbers themselves do not seem that scary, but there are particular factors that make this threat somewhat more severe:

- How many people's identities is one staff fraudster capable of compromising? Depending on the position of the individual concerned, it could range from a handful of specially selected identities through to thousands or even tens of thousands) of potential victims of identity fraud.
- These figures merely count the number of *proven* cases across the CIFAS Staff Fraud Database. There are currently over 130 Staff Fraud Members, so there are clearly a large number of organisations outside membership who are likely to be suffering the same kind of internal attack. It is not unreasonable to assume that these organisations, too, are seeing similar increases in this type of fraud to those inside the membership – it's just that these frauds go unrecorded. More concerning is the number of such frauds that not only go unrecorded, but entirely unidentified, thus leaving the perpetrator free to carry on compromising the identities of their employer's customers.
- These figures do not take into account those individuals who have been threatened and coerced into passing on client information to criminals.

More concerning is the number of such frauds that not only go unrecorded, but entirely unidentified, thus leaving the perpetrator free to carry on compromising the identities of their employer's customers.

For a case to be recorded on the CIFAS Staff Fraud Database, a criminal offence must have occurred; and if the individual was acting under duress, then they are not considered to have committed a criminal offence.

These criminals may keep looking, but will they still be able to find their men or women (but mostly men – two thirds of recorded cases are men) on the inside? The answer is probably yes - they will. It could be argued that if the country continues to climb out of recession, some confidence will return, and there may be fewer people willing to accept money from criminals to disclose personal data. That said, there is the small matter of a budget deficit to be addressed – through measures like a proposed increase in Vat (in the UK), which means that people's pay won't go as far. This could lead to those of a more susceptible disposition feeling the urge to augment their spending power by selling a bit of data on the side.

This, of course, assumes that these people are being motivated by feelings of financial desperation, which may be true in some cases – but it could just be plain greed. And let's be honest, your personal spending power is neither here nor there if someone is threatening the safety of you or your family. It should also be remembered that it's not always a case of seemingly honest people going rogue. There will also be those career criminals happy to take up employment with the sole aim of compromising data for their criminal colleagues. So yes, it seems fair to say that there will always be a supply of people whom organised criminals can use to obtain data – willingly or otherwise.

The upshot of this is that the problem and harm caused by staff fraudsters who compromise customer data is unlikely to go away any time soon. This means that unless organisations can effectively prevent these frauds from occurring, they will have to cope with the risk of the reputational damage caused by corrupt staff, and the financial fallout caused by the fraudulent attacks made by the criminals who receive the data. Neither should those whose details have been compromised be forgotten. The innocent victims of these identity crimes will be forced to spend time and money unravelling the mess that the criminals have made of their financial identity as well as suffering the emotional trauma of having their good name abused.

Examining Motivations for Internal Attack

Introduction

In the mid 1940s, Donald Cressey, an eminent criminologist, introduced the 'Employee Fraud Triangle' – showing the three

ARTICLE— CIFAS CONT...

constituent parts of an employee fraud: **Rationalisation, Opportunity and Motivation.**

It can be difficult to predict an individual's self justification, and opportunities for attack are already the focus of most anti-fraud controls - but motivation is never really considered. This may be a mistake as there are certainly areas where understanding the reasons behind a major attack could enhance prevention and detection, and help to identify an individual's predisposition to attack.

Studies and Comment on Motivation

A 20 year study (Hollinger & Clark) of 12,000 employees concluded that the most common reason for employees committing fraud had little to do with **Opportunity** but more with **Motivation**. The KPMG *Profile of a Fraudster Survey (2007)*, meanwhile, showed the main motivations to be financial pressure, often from an excessive lifestyle. No studies, however, have examined the breadth or depth of motivations, nor their potential relevance in internal fraud/crime management.

Types of Motivation

Another American criminology commentator (Nettler) succinctly summed up the types of motivation as: "Babes, Booze and Bets". While tongue in cheek, this does cover a large proportion of motivations, but by no means all: so a closer, more exhaustive, examination is worthwhile.

There are probably three major fields of motivation (all with some cross-over) which are outlined:

1. Greed

2. Need

- a) Debts (self inflicted)
- b) Debts (true necessity)
- c) Targets/Survival/Concealment of Error/Deficit
- d) Coercion/Threat/Blackmail
- e) Addiction: alcohol, drugs, sex, gambling

3. Miscellaneous

- a) Malice/Revenge (Existing)
- b) Malice/Revenge (Responsive)
- c) Competitive Sabotage
- d) Peer (or Family) Pressure/Loyalty
- e) Psychological Problems
- f) Excitement/Entertainment/Self-Aggrandisement/Ego
- g) Idealism/Terrorism
- h) Stupid/Naive (i.e. no deliberate motive)
- i) Mole/Cell (i.e. only purpose to employment)
- j) Industrial Espionage

A lot of these are known to us, and we will commonly see cases exhibiting some of the features. It is worth recording, however, some examples of the less obvious ones to illustrate that all can be dangerous if ignored.

2d there has been a very recent manifestation (trial June 2010) where a bank cashier helped thieves steal £150,000 after they threatened to uncover her as a bigamist.

3a, 3g, and **3i** are exemplified by a case in 2006, where alleged terrorists were taped discussing 'targeting utility companies by using recruits with inside knowledge to cut off electricity, water and gas power supplies across the country'.

ARTICLE— CIFAS CONT...

An unusual example of **2a** (and possibly **2e**) is the case this year of the NHS Trust employee who stole £200,000 from various Trusts to fund her purchase of 18 show-jumping horses.

In 2006, a Loans Manager for a major bank defrauded £21 million and at least part of his motivation was thought to be self-aggrandisement (**3f**); looking good to his friends and rugby club associates, as well as some element of **2c**. Probably the most famous example of **2c** is Nick Leeson (Barings), as well as the recent allegations against a French trader.

Motivation Linkage

It is possible to link most motivations under four main Risk Factor Indicators (RFIs):

- Financial – **1, 2a, 2b, 2e, 3c, 3j**
- Compulsion – **2c, 2e, 3a, 3b, 3e, 3g, 3h**
- Secret/Embarrassment – **2d**
- Illogical – **3f, 3i**

There are opportunities to detect these RFIs in both subjective and objective controls before and after employment. It is worth looking at the most difficult of these first.

Vetting (Pre-employment Screening) Control

To spot RFIs will necessitate detailed 'checks' and realistically we can only conduct that level on approximately 10- 15% of roles. It is necessary, therefore, to decide which posts have a high risk.

There are processes whereby one can measure attack opportunity, ease and impact for each role (or role family). This not only enables proportional (most common legal test for 'intrusive' vetting) and targeted vetting controls but also allows the same resource focus for many of the other controls (see below).

In order to detect RFIs it is important to ensure that the following points are covered in a vetting exercise:

- Is their application real?
- Are their qualifications (if true?) consistent with their career path to date?
- Is what the subject does, or has done:
 - A secret (e.g. criminal record, a habit or extra-marital affair)?
 - Expensive for them?
 - A risk because of how often or how much they do it?
 - Embarrassing if revealed/ discovered?
 - A risk to them or anyone else?

Vetting, of course, is a huge subject in itself, but it is important to understand the legalities within your particular jurisdiction. It is not only possible to screen for motive presence but also feasible to discover any propensity or capability for fraudulent/ criminal activity.

The Key is to look for the unusual or the inexplicable.

The analysis for RFIs must take into account all subjective as well as factors e.g. too much money can be as much an RFI as too little and one man's gambling addiction is another's hobby. For example: a £100 a week gambling habit may well pose a risk for a clerk who is only able to earn £20k pa (possible addiction), but it is not a risk for a Director who is to earn £100k pa (probably more a hobby) – unless ...he has kept it a secret from his wife?!!

(NB. Such detailed (Gold Standard) screenings must be conducted by experienced investigators. This is particularly important in the interviews and analysis of data e.g. bank accounts.)

General Controls

Whether the motivation or RFI is 'vettable' or not – all motivations and the resultant product are controllable:

ARTICLE— CIFAS CONT...

1. Education and Training – Security Awareness Programme
2. Professional Investigative Capability and Well Publicised Deterrent
3. Fraud and Theft Detection
4. Communication and Intelligence
5. Audit Trails, Logs and Reconciliations
6. Monitoring and Exiting of High Risk Posts
7. Segregation and Compartmentalisation
8. Access (Logical and Physical) Controls – particularly for High Risk
9. Information (not just IT) Classification and Protection
10. Foster Good Industrial Relations
11. Realistic Target Programmes
12. Duty to Report – not just whistleblowing, but a mandatory duty Moreover, it should now be obvious that each of the above controls is better applied with knowledge of the range of Motivations and their RFIs.

Conclusion

Making the connection between why employees commit employee fraud and applying controls respectively has to be more effective than simply having controls based on how attacks are perpetrated. That said, I don't believe this is something that will provide easy wins in the short term - but what is certainly evident from the above

A Case Study

Candidate supplied CV, references, bank and financial outgoing statements. Examination of the documents and the candidate revealed RFIs of a predisposition to fraud/crime, namely a drug habit (uncovered by spotting inexplicable cash withdrawals every second Thursday) and forged references (same misspellings as in CV) to cover a dismissal for alleged bribery. It is not always feasible to spot some motivations prior to employment, e.g. when it is a first time offence and the employment is itself causal to the Motivation (3a) and presents the Opportunity and, if necessary to the miscreant, the Rationalisation.

Almost all motivations would become 'vettable' if we applied repeat vetting (on High Risk posts). Repeat vetting would be particularly successful if linked with Fraud Monitoring/ Detection and other objective post employment controls.

THANK YOU TO CIFAS – THE UK'S FRAUD PREVENTION SERVICE FOR PERMISSION TO USE THIS EXTRACT FROM THEIR REPORT— "THE INTERNAL BETRAYAL". FOR FURTHER INFORMATION PLEASE GO TO Website: www.cifas.org.uk , www.identityfraud.org.uk

SAICB STAFF VACANCY - INVESTIGATIONS MANAGER

INVESTIGATIONS MANAGER

The South African Insurance Crime Bureau (SAICB) has a vacancy for an Investigations Manager, who will need to meet the following criteria:

Responsibilities

Assume full leadership responsibility for the investigation arm of the SAICB which will entail overseeing the investigators and analysts, and all cases being handled by the SAICB.

SAICB STAFF VACANCY - INVESTIGATIONS MANAGER *CONT...*

Providing overall leadership and direction for investigations and analytical processes.

Monitoring and directing of all investigators and analysts

Overseeing team development and performance.

Liaise with all relevant participants of the investigation including SAPS and NPA, and other government departments, etc.

Build relationships with relevant stakeholders and parties instrumental in the finalisation of investigations.

Provide feedback to COO on all current investigations and operational requirements on a regular basis.

Qualifications

Matric and relevant tertiary qualification

FAIS Accreditation or a FAIS recognised qualification will be highly beneficial.

Leadership, management and or Insurance related studies completed or in progress will be beneficial.

Relevant criminal and related legal courses.

Management courses

Experience

Investigation experience within the short-tem insurance industry for at least 5 years in a senior capacity is required.

Previous experience in either motor, non-motor, business, salvage and/or fire investigation will be highly beneficial

SAPS/investigation experience

Management experience essential

Experience using advanced methodologies and technologies

Skills and Competencies

Technology focussed management and investigation techniques

Leadership and management skills are essential

Excellent administration and organisational skills

Excellent interpersonal and communication skills (verbal and written)

Self disciplined and self motivated

Problem solving/initiative

Negotiating

Stress/change tolerance

Tenacity and resilience

Be an analytical thinker

Customer service oriented

Deadline and results oriented

Attention to detail

Takes ownership and responsibility

Adaptability

Conflict handling

Strong sense of self and purpose

Salary is negotiable and dependant on experience. Please send your complete CV with traceable references to Melanie Pillay on melaniep@saicb.co.za or fax: 0866 317 796, by latest, Friday 15 April 2011.

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