Editorial…

Welcome to the 1st issue for 2014!

My apology for the delay but 2014 has been a busy year but we are back on track with the newsletter!

While on vacation during December 2013 I read the following press article:

Rainbow nation or not, South Africa is battling a crime epidemic.

And when we returned at the beginning of January, the first article I see is: 2014: a Good Year for the Fraudsters!

The article discusses how government and law enforcement in the UK are struggling to tackle the fraud issue and that fraudsters feel quite optimistic about the year ahead. If that’s the scenario in the UK I think the fraudsters in South Africa must be ecstatic about 2014!

Then in February we see this article: “South Africa is the world leader in Money-laundering, Bribery & Corruption, Procurement fraud, Asset misappropriation and Cybercrime.”

What does 2014 hold for your organization – will you be another fraud statistic or do you have the determination to actively fight the fraudsters who are targeting your organization?

This newsletter provides world-class articles that can assist forward-thinking organisations to stop the bleeding of profits to fraud and to have a healthy, profitable organization.

Here’s your opportunity to read & learn & to attend training courses to acquire the skills needed to deter fraud & corruption…

In This Edition:

- 6 Common Myths about Fraud
- What % of Employees are Stealing?
- Shizaru Fraud Surveys
- What can Cyber Fraud Teach You about Preventing Insider Fraud?
- NYAWO NTATHU – the 3-legged approach to Fraud Prevention
- ID Theft – are You at Risk?
- ReportLine – A new Whistle-blowing Service
- The UK Bribery Act
- Social Media Risks
- Fraud Awareness Training Courses

Enjoy!

Mario Fazekas, Editor
Email: mario.fazekas@exactech.co
Mobile: + 27 (0)83 611 0161
www.exactech.co
6 COMMON MYTHS ABOUT FRAUD

If not debunked, they can obscure the existence of white-collar crime.

(Based on an article written by Joseph Wells and printed in the AICPA’s [American Institute of Certified Public Accountants] Journal of Accountancy).

A solid auditing or accounting background is helpful in uncovering white-collar crime, but it's not the whole answer. Auditors now turn up only about 20% of the frauds detected. Most fraud cases are discovered by accident or are revealed through complaints by co-workers.

Globally, employees are stealing as much as $3.5 trillion annually, according to estimates from the Association of Certified Fraud Examiners (ACFE), which specializes in fraud detection and deterrence. They also show that the average bank robbery nets the criminal only about $3,200, but the average bank embezzlement is $125,000. ‘Internal Controls’ do NOT equal ‘Fraud Prevention’, so to meet their expanded responsibilities to uncover fraud and control it, CPAs need to know more about fraud prevention. In particular, they need to debunk these six myths about fraud.

MYTH no. 1 - MOST PEOPLE WILL NOT COMMIT FRAUD

The notion that most people are immune to the temptation to commit fraud is probably the biggest myth of all about financial crimes. Fraud perpetrators come from all walks of life, all economic circumstances and all social classes. The public at large, including CPAs, has trouble coming to grips with a fact of life: Some people lie, cheat and steal. Sociologists suggest the reason is instinctive—to receive rewards or avoid punishment. The greater the promise of reward and the less the threat of punishment, the higher the motivation for antisocial behavior.

McKinley was about as unlikely a thief as you could find. A CPA and the only son of a judge, he had attended the right schools, worked at a large national accounting firm and married well. McKinley eventually went to work for the right bank as chief financial officer, where he proceeded to steal $100,000 right under the internal auditor's nose.

In McKinley's case, as in most frauds, it was a combination of three factors: motive, opportunity and a defective set of values. He was in a financial jam and decided to "loan" himself out of it. He simply moved the money he needed to a checking account he controlled and charged it to the bank's expense. It certainly would have been easy enough to find if the internal auditor had suspected the theft because the trail was there.

The late Donald Cressey, a noted criminologist, pioneered the study of embezzlement by interviewing approximately 300 prison inmates in the 1950s. He showed that the fraud perpetrator is normally caught up in a complex web of circumstances. Cressey discovered that nearly all fraud perpetrators have three things in common: a motive or pressure, which he defined as being usually a hidden or "unshareable" financial need; a perceived opportunity to
commit fraud without being detected (usually caused by weak controls); and an ability to **rationalize** the theft. This is normally done by calling the theft something else—for example, “borrowing” from the company to get out of a financial bind. Cressey said fraud occurs only when these three factors (known as the Fraud Triangle) are present at the same time. Luckily, this does not happen too often.

W. Steven Albrecht, president of the ACFE and an accounting professor at Brigham Young University, noted similar characteristics in a study of 212 fraud cases: The motive is usually financial, the opportunity is there and the person is able to compromise his or her integrity.

Opportunity almost always relates to position. Managers are no more or less honest than the employees—they just have more opportunity to commit bigger thefts. In McKinlcy’s case, it was a common pattern: excessive leverage, marital problems and too much control. Yet had the internal auditor not fallen for the first myth, he might have at least known whom to look at, if not where to look. Considering there are almost countless ways to defeat internal controls, knowing who to suspect of fraud is critical to its detection.

**Fact**

Most people can and will commit fraud—under the right conditions. We have found the “Pareto Principle” to be most relevant here: 10% of people are honest, 10% are dishonest and 80% sit on the fence and could go either way depending on their circumstances. Keep in mind that the greater the promise of reward and the less pervasive the threat of punishment, the higher the motivation to defraud.

---

**What % of employees are stealing from their employers?**

Whenever we do presentation to boards we discuss the Pareto principal (80/20 rule) where we say that 10% of employees are honest, 10% are crooks and 80% could go either way, depending on factors such as the control environment.

A few years ago when I did the presentation for the board of a mining house, the CFO was most offended by these stats and he said that it is impossible for 10% of his employees to be thieves/dishonest/unethical/corrupt and preposterous to even consider that some of the 80% could also be crooks.

From what I have seen over my 20 years in the forensic field I stick by this 80/20 principal as a general rule but in the USA, a survey, conducted by Forensic Accounting Firm Kessler, found that **95%** of employees could be stealing from their employers! They surveyed staff members and found that the theft not only includes office supplies, equipment and company products but much stolen time and the theft and sale of corporate secrets. You can view the video [here](#).

With the advent of technology, nearly 80% of those surveyed admitted to using company computers and phones for some sort of personal activity while at work. One of our clients here in South Africa, monitored their employees’ computer usage over a month and found that
between 50-80% were spending up to 4 hours per day on Facebook, Twitter or other social media during work hours!

Many employers think these types of activities are minor but they do add up and minor ethical breaches tend to progress to major ethical breaches.

How does one employee steal US$1.8 million?

Easy – steal an average of $800 per day every week-day for over 8 years! Judith Oakes worked as an accountant at a school in Los Angeles and she was responsible for overseeing the counting of the lunch money each day that was taken in at the cafeterias.

How did she manage to steal this money each day with other people in the room? **She stuffed the money down her bra when the others were not looking - fraud does not have to be sophisticated to be effective!**

After an audit was done it was found that **$3.1 million** was missing over the past 11 years. I wonder if this was the only audit done on the lunch takings?

Lunch money is not high on the priority list of most organisations but look at how these small daily losses added up! Judith worked at the school for 25 years and lived a lavish lifestyle on a modest salary.

‘What you don’t know can hurt you!’

Exactech have teamed up with Zetta Solutions to develop a sophisticated web-based **survey tool** that can get effective feedback from your employees in a totally anonymous and secure environment.

You have a choice of a fraud, ethics or corruption survey with standard questions or we can insert questions of your choosing.

For further information contact:

Carl Venter at 082 784 3439 / carl@zettas.co.za

Mario Fazekas at 083 611 0161 / mario.fazekas@exactech.co
What Can Cyber Fraud Teach You About Preventing Insider Fraud?

by Mike Hopkin

Earlier this year, federal prosecutors charged five men in the largest cyber fraud case ever filed in the United States. The offense? Theft of credit and debit card information that cost companies - many of them blue chip enterprises - more than $300 million.

And while none of the alleged perpetrators were company insiders, the case still holds many lessons for organizations that have grown complacent with inadequate or non-existent insider fraud prevention policies.

Unauthorized access comes from unexpected sources

Most companies targeted by the cyber fraudsters were big, consumer-facing brands like J.C. Penney, JetBlue Airways, and Carrefour SA. These organizations likely never expected a small network of hackers from Eastern Europe to breach their sophisticated security frameworks, all of which were presumably up to industry standards.

But breach them the hackers did. Unauthorized access, it seems, can come from the most unlikely of sources - and the same holds true for insider fraud.

Who commits insider fraud? More often than not, it’s longtime employees with authorized access to sensitive information. They’re the people management trusts; sometimes, they’re the managers themselves.

While many professionals find it hard to believe their fellow colleagues are capable of stealing from their employer, it’s the truth. And according to the most recent Ponemon Institute study of insider threats, the fraud risk posed by this type of employee is on the rise.

Witnesses often protect the guilty

Of the five men charged in the cyber theft case, three remain at large and may never face extradition. That’s presumably because certain Eastern European governments either ignore or harbor cyber criminals whose skills they consider an asset to their national economies.

But just as some countries tolerate cyber fraudsters’ illegal activities, witnesses to insider fraud often do exactly the same thing.
When a witness is subordinate to a guilty party within the corporate value chain (e.g. somebody sees his or her boss committing fraud), the theft may go unreported. This is frequently the case when the insider threat comes from a manager or board member. Even if the perpetrator commits fraud in a relatively open manner, observers may keep quiet for fear of retribution.

**Prevention remains key**

Catching the European cyber criminals didn’t happen overnight; law enforcement spent years trying to find them. And in the meantime, the illegal activity only escalated.

The lesson? Fraud - whether it comes from cyber criminals or company insiders - often continues after it’s discovered. Whenever possible, preventing the fraud from occurring in the first place is preferable to waiting around for it to happen. Opt for the latter and your organization could face months of lost revenue, not to mention a costly and time-consuming investigation.

Consider the numbers. On average, it takes organizations 87 days to notice fraud is occurring. After that, they spend another 105 days trying to discover the responsible party. All told, that’s more than six months of on-going insider theft! Why not take steps to avoid the inevitable income loss and possible brand damage inherent to this type of fraud?

Doing so could save your organization millions in the long run. You’ll boost your competitive edge, too.

**Mike Hopkin**

Michael manages the enterprise fraud management and compliance products at Attachmate. He has more than 17 years’ experience developing and designing information technology, security and compliance applications. He’s currently focusing on bringing industry leading products to market for internal fraud, privacy monitoring and compliance for health care and financial organizations. Michael blogs regularly on topics of leadership and product management, and his published articles and podcasts are recognized internationally.

Source: Insider Fraud Spotlight is the official blog of the Attachmate Luminet enterprise fraud management software product group.
NYAWO NTATHU

THE THREE LEGGED APPROACH TO FRAUD PREVENTION

Let me first explain the meaning of the wording NYAWO NTATHU which is Xhosa for the three legged cooking pot. Now it is common cause that should one leg of a cooking pot break then the pot falls over and the contents are spoiled.

This has led me to the belief that in order to prevent or at least reduce the exposure to fraud and financial crime in organisations, there has to be a three legged approach, namely

1. Governance
2. Risk Management
3. Ethics and morals.

The reader will note that I have omitted the word Corporate in the context of Governance. I suggest that Corporate Governance in many organisations stops at the Boardroom door and from my experience I have noted that the requirements of good governance seem to flounder in many corridors of power and never reach the operational level of the organisation.

However, before I discuss the elements of my proposed three legged approach to fraud and financial crime prevention let me ask the reader one question and this relates to what is commonly called the “tick box approach” to fraud and financial crime prevention adopted by many organisations and often used by internal audit.

My question is simply “If the tick box approach works why is fraud and financial crime increasing at unprecedented rates both here in South Africa and globally?” If I may answer my own question and use NYAWO NTATHU as my example;

- Governance is not working at all levels of the organisation
- Risk Management is not always an independent function within the organisation reporting directly to the Audit Committee and can often be downplayed by Executive Management protecting their own position and the identified risks to fraud and financial crime aren’t being heard in the right places, especially when the identified risk reflects adversely on Executive Management.
- The “Tone at the Top” is a very hackneyed phrase but so very applicable in many organisations where the “wink wink..nod nod” philosophy still applies when it comes to ethical conduct and moral behaviour in the organisation. Can Executive Management justify the free tickets to the rugby or cricket or the weekend visit to the game park and not expect employees in the organisation to adopt an attitude of “what’s in it for me?” There is ample evidence to show that unethical behaviour by senior and executive management in organisations is one of the biggest threats to risks of fraud and financial crime taking place.

So how do we re-think the approach to fraud and financial crime prevention utilising the NYAWO NTATHU philosophy and ensuring that all three legs of the pot are firmly in place in the organisation and the pot is not going to spill over and spoil the contents.
Governance

- As I indicated earlier, I have left out the word Corporate deliberately because I believe that the focus must be on Governance across the whole organisation. There is no doubt that the King Corporate Governance reports are possibly, if not, the best in the world but as I indicated earlier, are these reports being translated into meaningful action at all levels. In support and complimentary to King I would propose that organisations might care to consider the Global Business Standards (GBS) Codex¹ which was developed from various Corporate Governance report from around the world by three eminent professors at Harvard Business School in the United States.

In essence the Codex suggests the following eight principles;

1. **FIDUCIARY PRINCIPLE**
   Act as a fiduciary for the company and its investors. Carry out the company’s business in a diligent and loyal manner, with the degree of candour expected of a trustee.

2. **PROPERTY PRINCIPLE**
   Respect property and the rights of those who own it. Refrain from theft and misappropriation, avoid waste, and safeguard the property entrusted to you.

3. **RELIABILITY PRINCIPLE**
   Honour commitments. Be faithful to your word and follow through on promises, agreements, and other voluntary undertakings, whether or not embodied in legally enforceable contracts.

4. **TRANSPARENCY PRINCIPLE**
   Conduct business in a truthful and open manner. Refrain from deceptive acts and practices, keep accurate records, and make timely disclosures of material information while respecting obligations of confidentiality and privacy.

5. **DIGNITY PRINCIPLE**
   Respect the dignity of all people. Protect the health, safety, privacy, and human rights of others; refrain from coercion; and adopt practices that enhance human development in the workplace, the marketplace, and the community.

6. **FAIRNESS PRINCIPLE**
   Engage in free and fair competition, deal with all parties fairly and equitably, and practice non-discrimination in employment and contracting

7. **CITIZENSHIP PRINCIPLE**
   Act as responsible citizens of the community. Respect the law, protect public goods, cooperate with public authorities, avoid improper involvement in politics and government, and contribute to community betterment.

8. **RESPONSIVENESS PRINCIPLE**
   Engage with parties who may have legitimate claims and concerns relating to the company’s activities, and be responsive to public needs while recognizing the government’s role and jurisdiction in protecting the public interest.

Each Principle offers a Key concept, a Constituency and a Standard to be considered for implementation. I have found that the GBS Codex provides an easy to understand and implement set of

rules and guidelines that can be developed and introduced at all levels in the organisation in simple language and without business jargon clouding the real issues.

➢ Risk Management

As one prominent author has said “Risk Management is not rocket science” and I certainly agree with him, providing you are not in the chemical or similar industry. However the focus of this article is fraud and financial risk management and numerous articles, blogs and LinkedIn comments and suggestions have been circulated globally on the prevention of fraud and financial crime. I am not going to bore the reader by repeating what has been said numerous times, but what I would submit is that there is one aspect of risk management that is not fully addressed in many organisations and that is the foundation stone of the process, namely risk identification and the management of a proper risk register. Again I must pose a question, namely “Where is your risk register kept and who has access to it and in what format is it?” The response I normally receive is that either (a) “I don’t know” or (b) “With the Chief Risk Officer”.

May I suggest that both of these responses require urgent attention. The objective of Risk Management is to identify ALL risks to an organisation and if staff don’t know how to either identify risk or report a risk exposure that they perceive, then the identification process is flawed.

I have found from experience that the development of a simple risk register on a normal spreadsheet and making it available on the organisations LAN for use by ALL employees to identify and report risks is one way of getting everybody in the organisation involved in the risk identification process and not just leaving this element to a few people. Not every risk reported through the LAN Risk Register will need to be escalated upwards and many can be dealt with and managed at the departmental level, but what about that little risk that an employee reports that when examined by the CRO and senior management turns out to be a serious risk exposure that nobody ever thought of.

The second aspect of risk management that I would like to talk about is that of disaster and recovery planning. Again, my experience has shown me that when I ask the question “Where are you going to work on Monday when you arrive for work and your office block has burnt down? 8 times out of 10 I receive the response “I don’t know”. What about the contents of the building or office block. How many computers, printers, desks, chairs, telephones and ancillary equipment can be destroyed if a fire ravages the building?

As an example let us consider an office block with 3 000 employees and 1 500 fixed terminal desktops. Has the company included in its Disaster and Recovery planning a method whereby 1 500 computers can be sourced within 72 hours.

I have serious doubts that a hardware provider keeps 1 500 computers on standby in their warehouse waiting for a disaster eventuality. However, a Service Level Agreement (SLA) with the supplier could include a requirement that in the event of a disaster the supplier will be able to source the required number of units from the manufacturer within a reasonable amount of time.

I use the above example to show that risk identification is the foundation on which an effective programme is based and this applies across the whole spectrum of risk including fraud and financial crime. Don’t leave it until the building burns down or the accountant has run off with the company funds.
My final comments on the risk management process relates to the future and how organisations need to prepare themselves for what is going to be an avalanche of fraud and financial crime across the spectrum of business. We are already seeing a breakdown in cross border financial transactions and Money Laundering is increasing at an alarming rate, especially in Africa. The previous President of South Africa, Thabo Mbeki stated some time back that Africa loses US$15 billion a year through “illicit export of capital”. Advanced technology in financial transactions, Nanotechnology and virtual currencies such as Bitcoin all pose tremendous challenges to organisations and their CRO’s.

My concern is that too few CRO’s are fully conversant with and able to identify the risks to fraud and financial crime that are going to pervade the market place in the months and years ahead. Organisations need to act now to (a) identify people with the appropriate skills and training who will be able to identify the new risks that are coming our way and (b) be able to introduce appropriate measures to manage down and eliminate those risks.

This is not going to be an easy task but if we do not face the challenges now I foresee many organisations being forced into bankruptcy, and I am not just talking about the small 100 employee type organisations. It is also pertinent to remember in our Risk Management planning that one of the biggest risk exposures that organisations are facing is the environmental issue and global warming, but this needs to be the subject of a separate excise other than to suggest that organisations start doing their homework now and don’t wait until the inevitable happens.

Ethics and Moral Standards

I can only repeat in this short article what Prof.Henry Mintzberg Cleghorn, Professor of Management Studies, Faculty of Management, McGill University, Montreal has said;

“Corporations are social institutions-communities. They function best when committed human beings work in cooperative relationships, under conditions of respect and trust. Destroy this and the whole institution of business collapses.

At the drop of the share price, even when the company remains profitable, out the door go all kinds of people—bones thrown to distract the hungry dogs of the financial establishment. Unfortunately, however these bones, or to use the actual vocabulary, “human resources” belong to flesh and blood human beings. Resources are things; they don’t mind being dispensed with. Human beings are people; they do. As they leave so they carry the data banks of their organisations with them”

These comments by Mintzberg epitomise the whole ethical and moral structure of an organisation or lack thereof. I submit that the final sentence of his comments could also include references to fraud and financial crime.

This article cannot go into the ethical and moral issues that face Executive and Senior Management on a daily basis. This would require far more space.

I merely want to ask the reader to truthfully answer the following;
1. I am always ethical
2. I am mostly ethical
3. I am somewhat ethical
4. I am seldom ethical
5. I am never ethical

And then to consider if the following applies:

1. I want to be valued
2. I want to be appreciated
3. I want to be trusted
4. I want to be respected
5. I want to be understood
6. I do not want others to take advantage of me

How you answer these points will clearly show whether your organisation has a strong ethical and moral culture and whether your organisation is exposing itself to fraud and financial crime.

The answers lie only with you as an integral part of your organisation and if you are prepared to implement the NYAWO NTATHU approach to fraud and financial crime prevention before adopting a “tick-box approach” to the problem.

If you haven’t got effective Governance in place, if you haven’t clearly identified your risks and if your ethical and moral culture is found to be wanting, the rest that follows is a waste of time and effort.

**Patrick Cunningham**  
Email: pat@cerberusrisk.co.za  
Cerberus Risk Consultants  
Cel: +27 (0)82 566 8999

Patrick Cunningham has been involved in risk management in its various forms for over 40 years  
Pat retired at the beginning of 2011 as Executive Director of the South African Fraud Prevention Service, a position he held from 2000 when he was appointed to start the service by the major banking and retail credit grantors in South Africa.

Pat is currently the part time Executive Director for Africa India and the Middle East for the ATM Industry Association (ATMIA). He also operates his own consultancy service providing conference presentations and workshop programmes in Corporate Governance, Risk Management, Ethics, Financial crime prevention and ant-money laundering.
Identity Theft – are you at Risk?

Banks, retailers, cellphone stores and travel agents are throwing clients' personal information in trash bins at shopping malls making it easy for fraudsters to steal identities, Saturday Star reported.

Bank details, credit card forms with signatures, copies of IDs and mortgage documents, all supposedly on their way to a landfill, were found in the bins.

Specialist fraud investigator Duncan Waugh took the newspaper on a tour of the bins.

There they found a number of documents, including a confidential affidavit to confirm an address with details of a home-owner, his ID number and signature along with certified copies of the client's ID, according to the report.

Then there were full details of an external transfer of money amounting to R400 000 with signed instruction forms, the ID copies of the sender, proof of address and the recipient's full details.

Areas where the personal and sensitive client information was picked up included Cresta, Rosebank, Sandton, Protea Glen and Southdale, the newspaper reported.

The information gathered was enough to allow fraudsters to open bank accounts, buy goods, illegally apply for credit, or access medical aids in your name.

Waugh said he believed the action of "raiding bins" was behind the country's identity theft.

"The big corporates are putting their customers at risk in direct violation of the Constitution's right to privacy," he was quoted as saying.

Source: News24

Editor's Note:

“DUMPSTER DIVING” is the practice of sifting through commercial or residential garbage to find items that have been discarded by their owners, but that may prove useful to the garbage picker. Dumpster divers will forage dumpsters/rubbish bins for items such as clothing, furniture, food, and similar objects in good working condition, but they also look for bank statements, credit card slips, and other documents that they can sell or use to steal your identity.

This is nothing new – about ten years ago we did a Fraud Risk Assessment for one of the large insurance companies - we put on our gloves and spent about 30 minutes going through their garbage, which was located unsecured on the street, and we found client signatures, bank statements, insurance portfolios and copies of client ID documents – all not shredded!
The need for a Whistleblowing Hotline

Extensive research has shown that the most effective way of exposing misconduct, dishonesty, asset abuse, safety & security risks and other ethical issues within an organisation is by implementing an anonymous hotline service. Establishing a hotline facility is a relatively affordable method for creating a reporting system.

Organisations need to recognise that a robust, secure and anonymous whistleblowing mechanism enables senior managers to detect and correct practices that may harm employees, shareholders, customers or clients. Unchallenged, such wrongdoing can reduce profitability, tarnish your reputation, demoralise employees, and result in substantial fines or costly lawsuits.

That’s why it is important for business leaders and employees to understand what modern whistleblowing is, how it can benefit them and their organisation and how it can be best implemented and managed.

Vital information can be gleaned from employees using a trusted, anonymous and independent channel for voicing their concerns. By not engaging the services of an external whistleblowing hotline, organisations risk creating long term problems that could have been identified and addressed here and now.

Most employees know about hidden problems in organisations, however they are often reluctant to come forward and report concerns to management or colleagues due to fear of victimisation or retaliation.

It is important that organisations educate their employees, so that they may understand that a whistle-blower is not a traitor, but is rather assisting in the protection of the organisation by reporting misconduct, which is a corrosive force that should not be tolerated.

ReportLine specialises in the provision of whistleblowing hotlines for organisations and operates 24 hours a day, 365 days a year. This hotline facility is a means for individuals to report unethical and illegal conduct in a safe, non-confrontational and anonymous way, which significantly increases the probability that concerned parties will come forward.
They differentiate themselves from their competitors in that they do not just provide you with a report of the information received, but their experts will also provide you with guidance on how you should deal with the information. Their experts are members of the Association of Certified Fraud Examiners, the Institute of Commercial Fraud Practitioners, the International Institute of Certified Forensic Investigation Professionals and other similar organisations that provide training to its members. Their forensic specialists network with other fraud specialists globally and can provide you with new fraud trends applicable to your industry and how to combat these.

Carl Venter, their Risk Executive, is a seasoned fraud risk management specialist with 34 years’ experience in combatting fraud and corruption. He and his team conducted investigations in most industries and can therefor provide you with valuable guidance on how to deal with the information received from the whistle-blower and you can contact them for guidance throughout the investigation process.

ReportLine works alongside your organisation’s Code of Conduct, promoting honesty, integrity and transparency and does not replace existing processes for raising concerns or feedback in the workplace but rather compliments these reporting mechanisms by providing an external independent reporting option to an organisation’s whistleblowing policy.

Whistleblowing information can be supplied to us via toll-free telephone, e-mail, fax, web-based reporting and mail.

They have a state of the art contact centre where access is controlled by biometric security. The server that runs the contact centre is independently housed in a fireproof room with an independent alarm.

ReportLine uses carefully designed systems, infrastructure and processes to protect your confidential and sensitive data. They use professional business standards, practices and technologies to secure, protect and preserve the integrity of data generated through our systems.

Their employees are thoroughly screened and are subjected to extensive background checks before they are permitted to work in our Call Centre. Call Agents are also subjected to regular truth verification testing (polygraphs) to ensure that they work with the highest level of integrity.

They operate with a zero-tolerance policy with regards to employee dishonesty or any other form of misconduct relating to integrity.

It is important that your staff members are regularly informed of the existence of the hotline and they will work with you to develop an on-going awareness campaign tailored for your organisation.

For further information contact Carl Venter at 082-784 3439 or visit the website
THE UK BRIBERY ACT AND WHAT IT MIGHT MEAN FOR YOU HERE IN S.A.

All businesses in South Africa encounter different types of human behaviour including corruption. As you may be aware, corruption is a criminal offence in our own and other countries. We therefore need to be aware of ‘anti-corruption laws’ elsewhere in the world which may affect our ability to conduct business in those countries or businesses that come from those countries. The business partnerships and relationships we have with other nations provide serious challenges regarding potential acts of bribery.

One of the toughest “anti-corruption laws” in the world is the 'UK Bribery Act 2010' that came into effect on 1 July 2011. This Act replaced UK bribery laws dating back to 1889.

The UK's anti-bribery act, unlike its counterpart i.e. the United States Foreign Corrupt Practices Act (FCPA), will apply both to acts of public and private sector corruption. There are no exceptions for so called ‘facilitation payments’. Both legislations have extraterritorial reach, which means that they apply to companies and persons outside of the territorial jurisdictions of their respective countries, which may have significant implications for South African companies doing business with UK organisations.

All individuals who are nationals of the United Kingdom or are ordinarily resident in the UK are liable to be penalised under the 2010 act for anti-bribery offenses. Furthermore, the Act also applies to organisations that are resident in the UK or conduct some part of their business in the UK. This would extend the application of the Act to any company that has a subsidiary or affiliate in the UK. Therefore, for example, if an agent of yours with a subsidiary in the UK, engages in bribery in any part of the world, it would render your company liable to prosecution in the UK.

One of the offenses of the UK Bribery Act which is important to all employees of SA companies doing business in the UK is the following:

“Failure (on the part of a commercial organisation) to prevent an ‘associated’ person from bribing another person with the intent to (i) obtain or retain business for the commercial organisation or (ii) obtain an advantage in the conduct of business”

This is a new corporate offense and it imposes strict liability with severe penalties such as fines or potential imprisonment for failure to prevent bribery by a corporate entity. Under this offense companies will be liable if anyone acting under its authority commits an act of bribery. Such persons include employees, consultants, agents, subsidiaries and joint venture partners. The only defence available to a company would be if it has put adequate procedures in place to prevent offenses of bribery and failure to demonstrate such compliance could expose you to potentially unlimited fines, as well as possible imprisonment of the Directors. Furthermore, a person’s acts or omissions done or made outside of the UK would form part of such offense if the person has a "close connection" with the UK.
It is important to note that any business in South Africa that has subsidiaries, joint business ventures, intermediaries, agents or sub-contractors to a UK entity will be bound by this legislation. Consequently, any South African company that carries on a business or part of its business in the UK must abide by the rules of the Act.

The penalties under the UK Bribery Act are severe; unlimited fines for companies, up to ten years in prison for individuals involved. In addition there will also be the danger of adverse publicity where a company is potentially investigated and prosecuted.

You should ensure you have adequate policies and procedures on maintaining an ethical culture, whether a stand-alone anti-corruption policy or part of your code of ethics.

All employees should therefore be required to comply with these laws at all times and should refrain from any such unethical and criminal conduct. But keep in mind that you must provide adequate training and awareness for your staff members in order to hold them accountable for such offences. In addition, you should have a "Zero Tolerance" approach to such behaviour, whether from a junior employee, or one of the executives, as it speaks volumes when a senior person is disciplined for contravening policies!

Ken Lesueur, CFE
Group Loss Manager
Adcock Ingram


IIA Namibia 2014 National Conference

The IIA Namibia is hosting their 2014 National Conference on 2nd June 2014 at Arrebusch Lodge in Windhoek.

The theme for the conference is "Driving Change and Delivering Results" with speakers from Bank of Namibia, Barnowl, E&Y, Exactech Fraud Prevention Solutions, CQS Technology Holdings, KPMG, PwC, Debmarine Namibia and more.

There are eleven exciting topics and Mario Fazekas will be speaking on Measuring the Ethical Environment of your Organization.

Please click here to download and view the program.
What is your organisation doing about the current *Social Media Risks*?

Organisations data is being compromised by staff members befriending total strangers and clicking on links from these ‘friends’.

This article entitled *[IT Guys Get Duped by Pretty Girl on Social Media]* sums up the situation very nicely. They created fake social media pages with a picture of a pretty girl and then sent friend and link invites out to the target organization staff members.

Within a day, their fake Emily had 55 LinkedIn connections and 60 Facebook friends, all with the targeted agency’s employees and contractors. Job offers came, along with offers from men at the agency to assist her in her new job.

Near Christmas the security experts placed a link on Emily’s social media profiles that linked to a Christmas card site they created. Visitations to this site led to a chain of events ending with the security team stealing highly sensitive information from the agency. Partner companies with the agency were also compromised.

The security people got what they wanted in just one week. The penetration scam was then done on credit card companies, banks and healthcare organizations with very similar results.

We did exactly the same thing last year for four clients to prove how vulnerable their systems were to penetration via social media.

In the first case we used a profile of a pretty woman and got over 135 friends, including the MD of the organization! For the second client we used a male and received only 13 friends so needless to say we reverted back to the pretty woman for the others and our friends were again in the hundreds!

Here are some questions for you:

- How far would they, or we, get if they targeted your organisation?
- Do you have a social media policy?
- Do you know what your staff members are posting or saying on social media?

We have compiled a 40-minute presentation on these social media risks and if you would like to have this presentation delivered at one of you management meetings please let me know.

Mario Fazekas | Email: mario.fazekas@exactech.co | Cell: +27 (0) 83-611-0161
Fraud and Ethics Training / Awareness Courses:

What have the Exactech team-members been up to?

Antonio presenting to the internal audit department of Massmart, now part of Walmart

Antonio posing with the Governor of Utah, Gary Herbert, and some of the ACFE Chapter members at the Utah Fraud Awareness Conference

and being interviewed by USA TV networks.
Mario did training for the following organisations:

- BICA (Botswana Institute of Chartered Accountants)
- Barclays Bank Botswana
- Federation of Swaziland Employers & Chamber of Commerce
- IIA (Institute of Internal Auditors)
- SAICA (SA Institute of Chartered Accountants)
- SA Reserve Bank

This was the feedback from the audience at the BICA Francistown Fraud Risk Management seminar:

<table>
<thead>
<tr>
<th>Rated Comments</th>
<th>Poor</th>
<th>Average</th>
<th>Good</th>
<th>Very Good</th>
<th>Excellent</th>
<th>Total # of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Material &amp; Handouts</td>
<td>-</td>
<td>2</td>
<td>13</td>
<td>12</td>
<td>7</td>
<td>34</td>
</tr>
<tr>
<td>Scope Of Content</td>
<td>-</td>
<td>1</td>
<td>10</td>
<td>13</td>
<td>11</td>
<td>35</td>
</tr>
<tr>
<td>Depth Of Content</td>
<td>-</td>
<td>2</td>
<td>9</td>
<td>17</td>
<td>7</td>
<td>35</td>
</tr>
<tr>
<td>Content Applicability</td>
<td>-</td>
<td>2</td>
<td>3</td>
<td>20</td>
<td>10</td>
<td>35</td>
</tr>
<tr>
<td>Presenter’s Performance</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>15</td>
<td>20</td>
<td>35</td>
</tr>
<tr>
<td>Presenter’s Knowledge</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>12</td>
<td>21</td>
<td>35</td>
</tr>
<tr>
<td>Presenters Interaction With Participants</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>14</td>
<td>18</td>
<td>35</td>
</tr>
<tr>
<td>Overall Session Rating</td>
<td>-</td>
<td>-</td>
<td>6</td>
<td>14</td>
<td>15</td>
<td>35</td>
</tr>
</tbody>
</table>

SAICA CFO Forum.

This was a new ‘round-table’ format that was a great success. The event was hosted in Sandton, Cape Town & Durban with a 2nd-round scheduled for July 2014.
Here are the dates for our popular 4-day *Fraud Prevention and Detection* course run by the IIA...

**22 - 25 July 2014, Bedfordview, Johannesburg**

Why these courses are important...

**According to the 2010 ACFE global fraud survey, the average organisation loses 5% of its annual turnover to fraud!!**

**General Course Outline…**

- The success of a fraud risk management program relies on an organisation implementing a dynamic and sustainable anti-fraud strategy.
  - We discuss criminology theory and the fraud triangle.
  - The three categories of occupational fraud are examined.
- We unpack the nine best-practice fraud prevention building blocks and then show how to get management buy-in.
- We use case studies; show DVDs and use practical exercises to ensure that workshop attendees are ‘edutained’.

Some past delegate comments…

- *Made me aware of the fraud risks to my clients and myself.*
- *I definitely enjoyed every minute and it was a big eye opener.*
- *Thank you for an excellent course - I was so impressed by your knowledge, presentation skills and enthusiasm.*
- *I am now able to go back to my company and plug the gaps.*
- *Made me realise that fraud is possible even if there are internal controls.*
- *It created a strong awareness in me on how to prevent and detect fraud.*
- *Mario has inspired me to go back and enhance our anti-fraud initiatives.*
- *Integrity and values must be the cornerstones to any organisation.*
- *The seminar was excellent and I greatly enjoyed the examples you provided of moral relativism, as well as the areas of vulnerability.*

To register please contact Jenine or Maria at the Events Department on:

Tel: +27 (0)11 450 1040, email: events@iiasa.org.za
Who do you trust to help protect your organisation's profits from Fraud?

“If you were to ask a group of typical accountants what deters fraud, they would respond in unison: ‘Internal control!’ Using this logic, companies with adequate controls would not have fraud. But they do, time & again”

— Joe Wells, founder of the ACFE

Internal Controls ≠ Fraud Prevention!!

Every organisation has internal controls but they don't all have fraud prevention!

Exactech specializes in helping private and public sector organisations to implement best-practice anti-fraud initiatives and offers the following services and products:

Fraud and corruption are ongoing risks for all organisations BUT this risk can be managed and therefore controlled. Many of our clients approach us after they have discovered fraud, normally by accident, but you have an opportunity to make use of our services to proactively prevent and detect fraud – as the saying goes: ‘an ounce of prevention is worth a pound of cure’!

www.exactech.co
The publishers believe that the information in this Fraud Risk Management Newsletter is correct. However, it is published without liability upon the publishers for loss of any kind occasioned by any person or organisation acting or refraining from acting as a result of information contained herein. Contributors’ opinions and statements should not be considered an endorsement by Exactech for any policy, programme or service. Subscribers, readers and users of all related services have been made aware that this publication is not a substitute for specific professional legal and other advice. Provided that Mario Fazekas (e-mail: Mario.fazekas@exactech.co) is notified of the intended use and on condition that acknowledgement is made to Exactech and the authors, you are welcome to reproduce articles.