



Editorial...

Welcome to the second issue for 2011!

The year started well for us as the fraudsters have not slowed down and some organisations are starting to get serious about protecting their profits!

It was also a great surprise this year when we listened to **Finance Minister Pravin Gordhan's Budget speech** where he made a special mention of Exactech and how Antonio has achieved such excellent growth for the company since he started it in 2007!

"The recognition by minister Gordhan shows we are doing something right. I have always wanted to make something happen, and the idea of being employed was not how I was going to make things happen," - Antonio Pooe.

It also seems like the cyber criminals have taken a liking to South African organisations as millions upon millions of Rands have been lost to cyber-frauds in the past few months. As a result, Exactech has acquired a stake in Ukuphepha Consulting (Pty) Ltd, an Information Security and IT Risk Management services company.

I had the pleasure of working with the directors of Ukuphepha when I was at one of the big-4 accounting firms so I know they get results - I think even the hackers are scared of them!

In This Issue:

- [How to Predict when People will Embezzle](#)
- [The Anatomy of Risk](#)
- [The CGF Pledge for Good Governance](#)
- [Cyber Fraud - Why are we still being Victimized?](#)
- [Ukuphepha - South Africa's Premier Cyber-Fraud Busters](#)
- [Integrity - what does this mean to you?](#)
- [New White Collar Crime book](#)
- [Fraud & Ethics Training Courses for 2011](#) - From July to October we are running courses with & for the IIA, SAICA, and CQS
- [Who do you trust to help protect your organisation's profits from Fraud?](#)

Enjoy!

Mario Fazekas, Editor

Email: Mario@exactech.co.za

Mobile: 083 611 0161

www.exactech-fraud-solutions.com

How to Predict When People Will Embezzle

...and How to *Stop* Them

Usually, three things must be present before someone commits fraud or embezzles...

- **Need.**
- **Opportunity.**
- **Rationalization.**

I call this the “triangle of fraud”.



The formula sounds simple, but when you think about the elements of each of the three triangle parts, the picture becomes a bit complex. The following guidelines may help...

THE NEED FACTOR

Need takes two forms—direct and indirect. **Direct need** involves stealing to resolve a desperate financial problem. Direct need is often driven by an addiction or compulsion—drugs, alcohol, gambling or an extramarital affair.

Indirect need, on the other hand, is a business owner’s or executive’s need. It typically is the need to keep the company afloat. This need results, for example, in cooking the books to make sure a loan is obtained or renewed—to buy time to fix a dire financial problem. Of course, it can also result in a host of other fraudulent acts, such as bank fraud, check fraud, invoice scams, etc.

THE OPPORTUNITY FACTOR

Opportunity is defined as a perception that there is a low probability of being caught. In accounting, the descriptive word for this is “poor internal controls.”

THE RATIONALIZATION FACTOR

Rationalization is the employees’ mental process of making his or her illegal action fit within a personal code of conduct or ethics. In other words, the dishonest employee must be able to “talk himself into the action.”

Rationalization often results in what I refer to as “situational fraud.” Employees’ propensity to steal or embezzle can be predicted on the basis of a widely accepted formula:

5% to 10% of employees would never—ever—do anything wrong. Another 5% to 10% of employees are always scheming (hopefully you don’t have many of these folks working for you). The real problem is the 80% to 90% of remaining employees who will commit “situational fraud”—fraud that results from being in a position to steal and easily rationalize the illegal deed.

Remember: Who are the only employees who can steal from you? **Answer:** Employees you trust.

This isn’t meant to imply that you shouldn’t trust employees. It simply means that you can’t afford to go lax on internal controls because you trust employees. Here are some warning signs and conditions where trusted employees may be tempted to commit situational fraud:

- A period when the organization is being downsized.
- Employees who are bored may steal for excitement.
- Employees make an honest mistake, discover a weakness in internal controls, benefit from it and are going to “pay it back.”
- Thrill-seekers who like bending the rules when the right situation presents itself.
- Employees who are under personal stress—with financial problems, divorce, serious illness (especially of a spouse, parent or child).
- Employees with addictions—to drugs, alcohol, extramarital affairs, gambling, etc.
- Employees who always have to be number one and/or can’t stand not being the center of attention.

ANTICIPATING CRIME

Modern CFOs know a lot about human behavior. For example, they know that behavior never remains static. **World-class CFOs understand that any time they change a reward, the compensation system or the control system, people will change their behavior to maximize the benefits of the change for themselves.**

Example: Many years ago automobile traffic engineers set out to reduce the accident rates at intersections. They set up cameras and videotaped the traffic patterns. At that time, the green light would turn red and the red light would turn green at the same time. But that one last car tried to get through while cars with the green light had permission to go. So the engineers changed the sequence to add a two or three-second delay (i.e., both lights stay red for that brief moment), giving that one last car time to go safely through the intersection. And of course adding the amber light soon became the standard for creating this delay.

The accident rate declined significantly for two or three months. Then what happened? Drivers coming to an intersection with a yellow light or just-changed-to-red light realized they had several extra seconds to make it through the intersection. Instead of one car going through on the red, now it’s three or four. The drivers adjusted their behavior to benefit themselves.

How does this apply to employee theft? When you change a system, policy or procedure, employees will change their behavior—sometimes in a dishonest way. You may solve one problem, but create an even worse problem.

So, what’s the solution? A sports metaphor may explain. Hockey players don’t skate to where the puck is, they skate to where the puck is going to be. So—to become effective at managing change without promoting crime, you must anticipate how employees—and executives—will react dishonestly to any changes, and correct for them.

MINIMIZING FRAUD

Sometimes vulnerability to employee theft can be reduced with a little creativity.

Examples:

- The owner of a small company with little segregation of duties can have the bank statement sent to his or her home, not to the company. To demonstrate his attention to the statements, the owner reviews them and then inquires about several items in each statement. This practice creates the perception that a theft would probably be detected, thus reducing the “opportunity” by increasing the risk of getting caught.

- Employees in a large company's purchasing department may set up phony vendor accounts with their own addresses. To deter this kind of theft, regularly match the employee address file with the vendor address file.
- Send a letter to banks where the company does business, asking to keep you informed whenever they open accounts using names similar to that of your company. If someone is stealing customer checks from AT&T, they might open an account under A&TT. The teller would likely accept the check for deposit assuming the company's customer simply wrote AT&T incorrectly.

Important: If you are an outsider—an accountant, auditor, banker, etc.—be aware that you may need to “sell” the importance of fraud deterrents from the bottom up...especially in small companies. Few business owners are eager to implement controls, because they don't want to send the message that employees aren't trusted any more.

The solution: Get one of the company's own employees—the bookkeeper or controller, for example—to ask for the change. Say, ***“You know, you have complete control of everything. You pay the bills, you make the bank deposits and you reconcile the accounts. If any money is missing, who do you think Sally (the owner) will suspect? For your own protection, you should get Sally to look at the bank statements and initial the envelope every month. I know she's busy, but it won't take her more than five or 10 minutes.”***

CONCLUSION

Business owners & CFOs must be aggressive about protecting the company's assets. You must understand how your internal controls, compensation & performance measurement systems drive employee behavior & structure these systems so that they keep the fraud triangle in check.

Source: Gary Zeune, CEO, [The Pros and the Cons](#), the only speakers bureau in the US for white-collar criminals. He has authored several books, including *The CEO's Complete Guide to Committing Fraud*.

THE ANATOMY OF RISK

Undoubtedly there is a risk in almost every facet of life; at the time when we were born, or when we decide to take a casual stroll in a serene park, or indeed when we make a decision to partner a new business venture or associate.

Although a person may not be conscious of the underlying risks that may await them when they, for example, decide to embark upon an enjoyable park outing, there could well be many potential or real risks awaiting our unsuspecting victim. Of course in most cases the victim will not have consciously calculated such risks, and managing them becomes that much more difficult.

Conversely, in a business environment, business leaders are expected -- as a matter of their fiduciary duties -- to act (severally and jointly) quite differently compared to the person in our previous setting. In fact, one can argue that in a business environment, business leaders need to have a certain foresight that enables them to predict, manage and mitigate against the likelihood of something negatively affecting the business, its operations and profits.

It is precisely for this reason, most particularly where shareholders have entrusted the company's management to serve and protect the assets of the company, that leaders are held accountable when things go wrong. Clearly this calls for leadership experience, good business judgment as well as the

necessary toolset to aide management decisions in an ever-increasing and complex business environment.

The word risk has its roots in the old French word risqué, which literally means “danger”; moreover it implies that there is an element of chance which is attached to the risk of a business (Littré, 1863). Interestingly the word “hazard” -- which has Arabic origins and is another term which is integral to the topic of risk and Risk Management -- can be associated with the game of chance, which was invented at a castle named Hasart, in Palestine, while it was under siege at the time (Oxford English Dictionary).

In his book, *Against the Odds* (1998), Peter Bernstein describes the manner in which risk evolved; in part due to the changes of thinking in the mathematical numbering systems which was based upon statistical probability and the rise in popularity of gambling. In essence, a move from the games of chance in Egyptian times (3500BC) which made use of the clumsy Roman numerals, was fully replaced by the Hindu-Arabic numbering systems and numerals 1,2,3 and so forth.

And so through the centuries, great mathematicians have concerned themselves with arranging data, establishing properties and rules to predict certain behaviour and events which could have negative (or positive) implications upon humanity, business and indeed our earth, which sustains all these fragile, symbiotic elements.

Increasingly, and most certainly after disastrous events such as 9/11 and the collapse of the world's economy (which was sparked by the breakdown of Lehman Brothers); business leaders are being questioned regarding their ability to manage risk. Outside of these questions, the legal systems worldwide are generally also beginning to hold business leaders personally accountable for their part in unscrupulous or reckless business activities, particularly when their actions result in unacceptable financial losses or worse so, the loss of life which is inflicted on innocent bystanders.

Whilst one would like to believe that business leaders prudently manage the businesses wherein we have invested our hard earned cash, the truth in many instances is that this may not necessarily be the case. As with many of the recent and spectacular corporate collapses, forensic audits have revealed a lack of proper controls, poor (or in some instances, no) risk management policies and reports, as well excessive uncalculated business decision taking, to name but a few reasons for the demise of so many organisations. One just needs to ponder the reasons why so many of the past corporate giants, which include **Enron, Worldcom, AIG, Bear Stearns, Atari, Netscape, America Online** and **Apple**, either no longer exist or have been significantly overtaken by their competitors? Indeed the same can also be asked of some South African companies such as **LeisureNet, Macmed, Saambou** and **CorpCapital**?

In short, one can argue that these former giants under-calculated their strategic and / or operational risks and for this they have paid handsomely. Hopefully business and its leadership have learnt from their past mistakes. In this regard, the **King III Report** on Corporate Governance - which sets out various accepted international business guidelines -- has been released for all companies in South Africa to adopt. Stakeholders may be assured that its contained business guidelines could serve as a catalyst to improve the manner in which the Board of directors will manage and report their risks, and be accountable for their deviation. **Of course receiving such guidelines is one thing, observing, and acting upon them and holding oneself accountable for not managing the risks of a business is altogether something else.**

“Managing risk is one of the things bosses are paid for, yet most companies still do not have any idea what is required of Risk Management,” stated The Economist (2004).

Terry Booyesen is the Chief Executive Officer OF CGF Research Institute (Pty) Ltd and can be contacted on Tel: +27(11) 476 8264, E-mail: tbooyesen@cgf.co.za, Websites: www.cgf.co.za, www.corporate-governance.co.za

The CGF Pledge for Good Governance - have you made your pledge...?

CGF Research Institute has been campaigning the **CGF Pledge for Good Governance** for the past five months and as expected, the long haul of this journey has *only* just begun.

Whilst many individuals have agreed this initiative is a critical requirement in an effort to combat the excessive corruption, greed and crime in our beloved country, their response to the call for action is very slow. And while CGF will continue this journey -- because they truly believe in it -- they have now also approached top business leaders and various government officials to reflect upon this initiative, and support it with their conviction. To date, they have sent both group and individualised invitations to literally thousands of business people and frankly, the responses to date have been very disappointing.

There is no doubt that with the new Companies Act 2008, which kicked in on 01 May 2011, companies will require far more astute business leaders to not only interpret the new Act, but indeed *follow* and *implement* it. Failing to do so, will most certainly bring personal and public liability to many. Hopefully, people will begin to realise that as business leaders, we are accountable to all our stakeholders and that each person -- increasingly -- will be called to attest their commitment to good governance practices.

“Each day, I see so much damage being done in our beautiful country - so much of it caused through idleness, complacency and of course exceptionally poor governance and a degradation of moral principles. The 'buck' rests with each one of us, and the change so many of us seek for South Africa, lies within us. I have often said that we cannot wait for our leaders of the country to cause change, each one of us can start the change from within.

My appeal to you -- if this is a cause you believe in -- is that YOU lead the way, by pledging yourself first. In doing this, CGF will at least have one extra individual who stands for Good Governance.

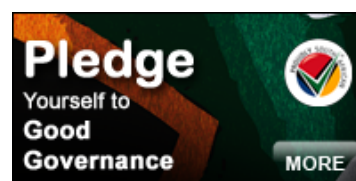
In time, others will follow your fine example and commitment for positive change.

CGF would be delighted to have you counted as a supporter of their Good Governance Campaign. The CGF Good Governance Certificate displayed upon your office wall will cause many others to think about your values which are not compromised by bureaucracy, neither complacency.

Each day that goes by, more atrocities occur whilst we remain quiet as we silently condone the thuggery in our country. Each pledge CGF receives, is yet another, and closer step toward a better life for all.”

Of course we need people of stature to support this campaign, but we also need ordinary everyday individuals to support this cause for good change. Perhaps the saying “*all for one and one for all*” is not that far from the mark?

I have made my pledge - have you...?



Please click Pledge Button above

Cyber Fraud: Why Are We Still Being Victimized?

By Peter Goldmann, CFE

The FBI recently announced its discovery of a new fraud scheme from China that targets businesses with bank accounts at local credit unions and community banks. These cyber criminals gain access to businesses' bank accounts through the computer of an unsuspecting employee from the targeted business.

Between March 2010 and April 2011, the FBI identified twenty incidents in which the online banking credentials of small-to-medium sized U.S. businesses were stolen and used to initiate fraudulent wire transfers to Chinese companies. As of April 2011, the total attempted fraud amounted to approximately \$20 million; the actual victim losses were \$11 million.

In a typical case, the computer of a person within a U.S. company with authority to initiate funds transfers on behalf of the U.S. business is compromised by either a phishing e-mail or by visiting a phony, criminally-operated website.

The malware implanted on the unsuspecting employee's hard drive collects the user's corporate online banking credentials. When the authorized user attempts to log in to his or her bank website, he or she is redirected to another web page stating the bank website is under maintenance or is unable to access the accounts. While the user is experiencing logon "issues," the fraudsters initiate the unauthorized transfers to commercial accounts held at intermediary banks, often located in New York. The stolen funds are then transferred to the Chinese economic and trade company bank account.

The unauthorized wire transfers have ranged from \$50,000 to \$985,000. In most cases, they have been above \$900,000. In addition to the large wire transfers, the FBI discovered that the malicious actors also have sent domestic ACH and wire transfers to money mules in the United States within minutes of conducting the overseas transfers.

Par for the Course?

This particular cyber fraud is interesting in and of itself, but that's not why I bring it to your attention. More worrisome, it is just the latest in a long string of cyber schemes that have been proliferating over many, many years, costing organizations of all kinds billions upon billions of dollars in losses. This particular scam employs social-engineering tricks as well as sophisticated malware. According to many cyber-security experts, social engineering-based crimes have, in the words of one such expert, "escalated significantly" in recent years.

Still, organizations continue to be victimized by a slew of technological attacks including the familiar hacking, virus, worm and Trojan horse attacks. Like the latest social engineering scams, all are aimed at illegally penetrating or bypass firewalls and other security defenses to steal either money or data or both. The latest headline-maker of course was Sony whose PlayStation Network was hacked, resulting in the theft of nearly 80 million personal records.

Why is This Still Happening?

It's almost as if we've become desensitized to these events due to their incredible frequency. But I'm betting that companies that have been victimized by the cyber-bad guys wished afterward that they had taken security just a bit more seriously prior to the attacks.

The \$64 million question is that, after all these years, why are organizations still falling victim in such large numbers to these now well-known schemes?

The answer is multifaceted. **In part, the primary targets -- SMB's (Small and Medium-sized**

businesses) -- are run by bosses far too busy to a) inform themselves about the threat, much less b) do anything to protect themselves and their businesses.

This is not a shocking new revelation. Almost by definition, SMB's lack the resources to implement and maintain the kind of state-of-the-art information system security defenses that large organizations can afford. But a \$900,000 cyber-ripoff can put some SMB's at serious risk of failure. **So you'd think that after all these years, management would bite the bullet, as painful as it may be to do so, in order to safeguard its financial and information resources.**

Another critical part of the answer is that senior executives of large organizations either don't want to deal with cyber-security or they are convinced their IT departments have the issue adequately covered. According to Lynn Goodendorf, CIPP, CISSP, CEO of Atlanta-based Good Security Consulting LLC, this mindset -- common in C-suites across industries -- results in a situation in which huge amounts of money are budgeted for technological security measures -- think firewalls and anti-virus software -- while other equally vital, non-technological aspects of effective enterprise-wide information security go unattended. Specifically, Goodendorf calls these "administrative controls". They include such critical activities as:

- Formulating and enforcing a clear cyber-security policy
- Implementing enterprise-wide cyber-security awareness training
- Strong password practices and procedures

Problem: As the sophistication of attacks increases, one thing is clear: If you ease up for one minute, your company and its customers stand to be the next victims.

Cyber crime is advancing at the speed of light. For example, Anthony Di Bello, product marketing manager for compliance and cybersecurity at Guidance Software Inc. a digital investigation service provider, was quoted on the website, www.searchcompliance.com as saying that his company has recently concentrated on designing cyber forensic technology to expose and address threats designed to evade layered security systems.

"Examples of these types of threats include variants of the ZeuS banking Trojan (a prominent culprit in the latest above-described account-takeover epidemic), criminal or state-sponsored malware, insider threats and even threats designed to affect critical infrastructure," Di Bello said.

Cyber-Social Engineering on the Rise

Meanwhile, attacks based on seemingly good old fashioned social engineering remain particularly successful because they rely on trusted insiders to introduce the malware into the network, Di Bellow added.

In a sobering indicator of how relatively low-tech cyber-fraud tactics continue to produce results for their perpetrators, Di Bello said that "[Social engineering attacks] could come in the form of an email from a supposed retailer with a 'click for some sort of promotion,' or an attacker leaving a USB drive on the ground in a public place near or at the target, waiting for a curious employee to plug the device into their computer, launching the payload."

Lynn Goodendorf says that these social engineering attacks are growing in both frequency and sophistication. And that is why limiting security resources to the technological segment of the problem is misguided. This is another key reason Goodendorf urges management to devote more attention resources to administrative controls.

Better Late Than Never

Goodendorf makes a strong argument for the theory that the continued deployment of social engineering schemes by cyber-fraudsters is that many senior executives continue

to back-burner the task of protecting against these attacks. Or they simply feel information security is too complicated and they delegate it, lock stock and barrel, to IT.

In a recent study of companies in Japan, it was determined that even organizations that do take the initiative to put tangible information security measures in place -- such as sophisticated security software -- still remain vulnerable to attack. **The reason, according to the researchers is that executives often fail to supplement these measures with "intangible" measures such as IT training and "continuous accumulation and sharing of knowledge" because they do not perceive the financial benefits of these actions.**

This, among many other factors, including predictions by cyber crime experts of a continued escalation of online crime, strongly suggests that **now is as good a time as any to stop procrastinating.**

Critical First Steps

There is a virtually endless variety of sources of reliable and non-technical recommendations for protecting your organization against hacking, social engineering attacks, malware and the other common cyber-crimes. Among the most succinct and current is the set of defensive measures contained in Verizon's "[2011 Data Breach Investigations Report](#)", a study conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit.

- **Achieve "essential", and then worry about "excellent."** Many organizations achieve high levels of security in numerous areas but neglect others. Criminals will almost always prefer the easier route. Identifying a set of essential controls and ensuring their implementation across the organization without exception, and then moving on to more advanced controls where needed, is a superior strategy against real-world attacks.
- **Optimize access control.** Change default credentials. When system/network administrators set up a new system, change the password. If you outsource this to a third party, check that they've changed the password. Don't assume that your staff or your partners consistently follow through on all policies and procedures. *Also important:* Along with changing default credentials, ensure that passwords are unique and not shared among users or used on different systems. This is especially problematic for assets managed by a third party.
- **Review user accounts on a regular basis.** The review should consist of a formal process to confirm that active accounts are valid, necessary, properly configured, and given appropriate (preferably minimum) privileges. Be certain as well to restrict and monitor privileged users: Trust but verify. Use pre-employment screening to eliminate the problem before it starts. And enforce segregation of duties to avoid having one employee capable of gaining unauthorized access. Make sure they know your policies and expectations and ensure that managers and supervisors are accountable for ensuring that employees adhere to them. *Also critical:* Keep a log of privileged use, with messages generated to management about these changes. Unplanned privileged use should generate alarms and be investigated.
- **Improve network security management.** Secure remote access services: In many instances, remote access services are Internet-facing. Instead, secure these services by enabling only specific IP addresses or networks to access them. Many organizations also allow any device on the network to connect and remotely access any other device. This is a serious security risk which should be remedied by tying down remote access services to specific management networks via access control lists.
- **Monitor and filter outgoing network traffic.** At some point during the sequence of events in many breaches, data leaves the system. By monitoring, understanding, and controlling

outbound traffic, your organization will greatly increase its chances of mitigating malicious activity.

- **Secure web development.** Include regular reviews of architecture, privileges, and source code. Incorporating a Security Development Life-Cycle (SDLC) approach for application development is recommended as well. Finally, help your developers learn to appreciate and write more secure code.
- **Log management and analysis.** System components called "logs" monitor traffic on your network if properly configured. By fully enabling so-called "application and network witness logs" and monitoring them you may be able to forestall an attack before it happens. Too often, evidence of events leading to breaches has been available to the victim organization but this information was neither noticed nor acted upon. Monitoring processes that provide efficient, and effective monitoring and response are critical to protecting data.
- **Define "suspicious" and "anomalous" and then look for what "it" is.** This can be vague, but generalizing what this entails in order to prescribe something for everyone would counteract the point. Determine what is critical, identify what constitutes normal behavior, and then set focused mechanisms in place to look for and alert upon deviations from normality.
- **Change your approach to event monitoring and log analysis.** Focus less on the "real-time" methods of detection, and more on the "this week" methods. Focus on the obvious things rather than the minutiae.
- **Increase awareness of social engineering.** Educate employees about different methods of social engineering and their potential origins. Too often, employees click on links they shouldn't and open attachments received from identified persons. Reward users for reporting suspicious email and sites and create the incentives necessary for vigilance. Train employees and customers to look for signs of tampering and fraud: such awareness campaigns have been around in certain areas for some time, but ATM and pay-at-the-Pump tampering/fraud seem to be increasing in number and scope.
- **Create an incident response plan.** If and when a breach is suspected to have occurred, the victim organization must be ready to respond. An effective Incident Response Plan helps reduce the scale of a breach and ensures that evidence is collected in the proper manner.
- **Administer mock incident testing.** This is another phrase for "practice" Practice makes perfect. Specifically, in order to achieve optimum information security, organizations should undergo routine incident response training that covers response strategies, threat identification, threat classification, process definition, proper evidence handling, and mock scenarios.

The Bottom Line

One of the many problems with information security today is that there are innumerable ways of perpetrating attacks, but there are also countless measures that can be taken to reduce exposure to these crimes. The trick, according to experts, is to know exactly what your vulnerabilities are and then go about finding and implementing the most effective countermeasures (this, unfortunately, does not include the critical step of putting a response plan in place in case you are victimized).

Achieving a level of information security that gives you enough confidence to sleep at night requires a powerful combination of financial, technological and professional resources... and a competent senior manager to ensure that they are properly deployed.

© 2011 White-Collar Crime 101 LLC, All Rights Reserved.

Peter Goldman is the author of [Fraud in the Markets: Why It Happens and How to Fight It](#), published by John Wiley & Sons, available at the [ACFE Bookstore](#). He is also the Editor and Publisher of the monthly newsletter, *White-Collar Crime Fighter*, <http://www.wccfighter.com/>.



UKUPHEPHA
CONSULTING

In the last four years, we've been able to position Exactech as the leader in Fraud Prevention and Computer Forensic Investigations.

During this time, it also became clear that there were certain gaps in the services we provide. One of these gaps was the provision of a Fraud Hotline service. This gap was closed in 2010 when we acquired stake in a contact center solution provider and launched the [Be Heard™](#) fraud hotline service.

The time has finally come for us to expand again, in an effort to offer our clients a holistic fraud prevention service. "Ukuphepha" a Zulu word, which translates to "comfort, safety and security", is the new addition to our stable of services. Ukuphepha Consulting (Pty) Ltd (aka UKU), will complement the existing Exactech services with a range of **Information Security** and **IT Risk Management** services that will provide clients with the mechanism of addressing these issues in a pro-active manner.

As the saying goes "...hindsight is the perfect sight...". With the inclusion of Ukuphepha Consulting, we aim to change this 'sight' from one of 'problem solving' to one of 'problem prevention'.

The Ukuphepha team is made up of dynamic and highly experienced Information Security and IT Risk and Governance professionals who specialize in the provision of value-driven services in the information security and IT risk management environment. They pride themselves in assisting organisations, regardless of industry, size or location, and believe in closely aligning themselves and integrating with clients, at both technical and managerial levels, thus adopting their "From the Boardroom to the Network" approach of providing seamless support.

The individuals associated to Ukuphepha Consulting have a broad knowledge base and have consulted and operated worldwide, ranging from countries such as the Far East, Australia, Europe, the United States of America (USA), and extensively across industries in South Africa.

They collectively hold a number of IT and Business degrees and certifications, with over 40 years of combined working experience in both the public and private sectors around the globe. Ukuphepha consultants become 'One' with the client, its environment and its people, and are looking forward to assist you and helping you achieving and realizing for you, leading and sustainable information security and IT risk practices, that are complementary to your overall business and technology strategies.

Our Services Now Include the Following:

<p><u>Governance & Compliance</u></p> <ul style="list-style-type: none"> • Industrial & process control compliance • IT support to internal audit • Corporate governance • King III implementation & compliance 	<p><u>Information Security</u></p> <ul style="list-style-type: none"> • Resilience testing & management • Governance, strategy & frameworks • Infrastructure assessments • Stielshield exec personal privacy 	<p><u>Information Management</u></p> <ul style="list-style-type: none"> • Data quality management • Data leakage prevention • Data privacy
<p><u>Business Optimisation</u></p> <ul style="list-style-type: none"> • Business process management • Service level management • Business optimization solutions 	<p><u>Strategic Services</u></p> <ul style="list-style-type: none"> • IT Strategy & Risk Management • Business continuity • Scorecard development 	<p><u>IT Fraud Management</u></p> <ul style="list-style-type: none"> • Cybercrime Forensics

For more information on these and other services we provide, contact any one of the following people:

- Antonio.pooe@ukuphepha.com
- Stieler.vaneeden@ukuphepha.com
- David.volschenk@ukuphepha.com



Integrity! by Mario Fazekas

'INTEGRITY' - most organizations have this as one of their values, which is commendable as integrity is a critical value for organizations that want to ensure honest, long-term business dealings.

During 2010 we rolled our many codes of ethics for companies and what struck us was that most employees, managers and directors did not know what their values meant! Some didn't even know they had values while others could recite the values correctly but could not tell us what integrity meant.

This proves the point that these codes of conduct and ethics policies must be **rolled out in workshops** so that all staff members can be trained and held accountable.

How important is Integrity?

In a survey of 54,000 people *Integrity* was by far the #1 **attribute** desired in a leader! (Quoted from Stephen R. Covey's preface to *Business with Integrity*).

What is Integrity?

Most people said that 'integrity' meant 'loyalty' or 'honesty'. Wrong! Some organizations have integrity plus honesty as part of their core values so they cannot mean the same thing!

According to Wikipedia, Integrity is a concept of **CONSISTENCY** of actions, values, methods, measures, principles, expectations, and outcomes. In ethics, integrity is regarded as consistent honesty and truthfulness or accuracy of one's actions. Integrity can be regarded as the opposite of hypocrisy, in that it regards internal consistency as a virtue, and suggests that parties holding apparently conflicting values should account for the discrepancy or alter their beliefs.

- At one of our clients, the HR manager received a complaint, after we had run one of our ethics workshops, from an employee who complained that I was '**trying to change her thinking**'. Well, yes, that is what I am trying to do - if staff members thought it was OK to lie, cheat and steal - it's not OK, and they should please change their thinking, beliefs and their actions accordingly!!
- At another fraud and ethics training workshop I was discussing the importance of integrity and a lady sitting right in front was shaking her head in disagreement. I asked her what the problem was and she replied "**You are asking for too much as we are only human**". I then asked her, as a human being, what amount of integrity she was capable of giving - her response "**Oh, about 90%**". I then went on to ask her if she was married, how long she had been married etc. and then I asked her if it was OK if her husband came home one night and said that he had been faithful to her about 90% of their married years? You can guess her answer can't you! "**I would divorce the scoundrel if he did that to me!**" Ah, so it's OK for her to give only 90% integrity but she then expects 100% integrity from others! I think that is termed hypocrisy!

We have found that **most** people do **mostly** right things **most** of the time and It's the difference between '**most**' and '**all**' where the challenge of doing right is found – and where the greatest opportunity for ethical enhancement exists.

To be sure, none of us is perfect. And that needs to be seen for exactly what it is: A FACT...A CONDITION, **NOT AN EXCUSE to do bad things**. Compensating for our imperfections and overcoming temptations we face requires commitment and self-discipline.

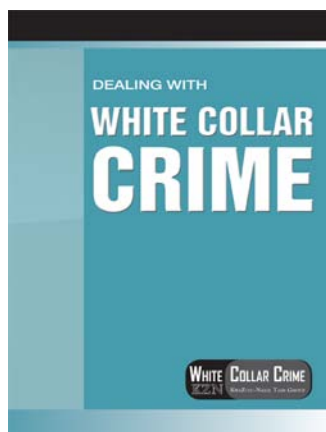
Would drink this glass of water?

If you pour a glass of water and add just one small drop of arsenic it will make you 100% dead as the water has lost its integrity.

What does Integrity mean at YOUR organization? Is it just another word or do you and your colleagues live by this value?

Please email [Mario](#) if you would like to discuss rolling out your code of ethics.

Dealing with White Collar Crime - the book every business should have!



White Collar Crime is estimated to cost the South African economy billions of Rands annually. As a result, never has it been more important than now for companies to be vigilant in preventing fraud.

Dealing with White Collar Crime, compiled by the KwaZulu-Natal Task Group, is available direct from the publishers, Contact Publications (Pty) Ltd, at R250, including VAT, plus R29 for packaging and local registered postage (total R279).

Each chapter is written by an authority in their field and includes a chapter on **Fraud Prevention** written by **Mario Fazekas**.

To purchase a copy please contact Contact Publications (Pty) Ltd. As follows:

Fax: 031 764 6974

Email: accounts@contactpub.co.za

Telephone: +27 (0) 31 764-6977

Suite 1, Fields Shopping Centre, Old Main Road, Kloof 3610, KwaZulu-Natal, South Africa.

For overseas postage rates and also bulk discounts for ten copies or more, contact Beryl Douglas at admin@contactpub.co.za

Fraud and Ethics Training / Awareness Courses:



Fraud Risk Management - are you winning or losing the battle?

- Monday 4th July 2011 - **Cape Town** CTICC
 - Tuesday 5th July 2011 - **Durban**, Suncoast Conference Centre
 - Wednesday 6th July 2011 - **Bloemfontein**, Protea Hotel
 - Friday 8th July 2011 - **Johannesburg**, Sandton Sun
-
- ***“Good venue, catering was excellent. Brilliant seminar, food for thought.”*** - Tabak Pelkowitz and Berman
 - ***“It is very well presented and the information is invaluable.”*** – Transnet Rail Engineering
 - ***“The best 2 speakers I've heard at SAICA training.”*** - Ogilvy

The programme will address the following critical issues:

- What is fraud?
 - How big a problem is fraud?
 - Who are the victims?
 - Who are the perpetrators?
 - What motivates the perpetrators?
 - Are there solutions?
- If yes, why is there still so much fraud?

To book your place please contact Pertunia as follows:

Telephone: 08610 SAICA or 08610 724 22

E-mail: pertuniam@saica.co.za

Website: www.saica.co.za

[Brochure](#)



Fraud Detection & Prevention Training Course - co-presented by CQS & Exactech

Why Should You Attend?

There is no other course in South Africa that combines both theory and ACL practical training; uses local and international case studies in the theory component to ascertain best practices and also covers practical audit tests.

You will Learn to...

- Perform data analysis tests to identify anomalies and policy non-compliance.
- Perform trend analysis on the anomalies to identify cause and fraudulent activity.
- Verify data quality and integrity.
- Examine data elements and table structures.
- Test transaction authorisation and validation
- Create tests for purchasing and payables, travel and entertainment expenses, and procurement card expenses.
- Describe Benford's Law and use Benford tests in ACL fraud analysis
-

Durban: 18 - 20th July 2011

Johannesburg: 23 - 25th August 2011

To book your place please click [here](#).



To download your free copy of **7 Steps to Tackle Fraud using Data Analytics** please click [here](#).



The Institute of Internal Auditors South Africa

Here are the dates for our popular 4-day *Fraud Prevention and Detection* course run by the IIA...

25 - 28 July 2011, Bedfordview, Johannesburg
18 - 21 October 2011, 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 Fraud Prevention Solutions specializes in helping private and public sector organisations to implement best-practice anti-fraud initiatives based on the nine fraud prevention building blocks.

Fraud is present in almost all businesses, with only the 9 fraud prevention elements and regular monitoring to keep it in check. When some of these elements are missing or are circumvented, frauds can quickly grow to shocking proportions.

Exactech specializes in:

- **Data Analytics**
- **Fraud Risk Assessments**
- **Code of Ethics Review / Compilation**
- **Policy Reviews**
- **Hotline Management**
- **Computer Forensics**
- **Fraud Awareness Training**
- **Ethics Training**
- **Fraud Prevention & Detection Training**
- **Cyber Forensic Training**

Fraud Risk Assessment	Accountability	Controls
Data Analytics	Policy	Whistle-blowing System
Value System - Ethics	Recruitment	Training & Awareness

Based on the ACFE Fraud Prevention Check-up

Contact: [Antonio Pooe](#) or [Mario Fazekas](#)
www.exactech-fraud-solutions.com

The publishers believe that the information in this Fraud Prevention 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@exactech.co.za)** is notified of the intended use and on condition that acknowledgement is made to Exactech and the authors, you are welcome to reproduce articles.