www.pwc.co.za/crimesurvey

Cybercrime in the spotlight

6th PwC Global Economic Crime Survey

South African Edition

November 2011

pwc

The PwC Global Economic Crime Survey remains the most comprehensive survey of its kind available worldwide.

Contents

Foreword

PwC conducts its Global Economic Crime Survey every two years. Separate reports are published by various countries, in addition to the overall global results report. I am pleased to present the South African edition of the Global Economic Crime Survey 2011. South Africa achieved a record 123 responses across 19 industry sectors. The large number and diversity of responses allows us to obtain a more representative data set which in turn produces a better picture of economic crime in South Africa.

As in previous years, the purpose of our survey is to inform South African business leaders on the continuously changing landscape of economic crime in our country and to encourage debate around strategic and emerging issues in this sphere. As you will no doubt notice, cybercrime receives focussed attention in the 2011 survey and we look forward to sharing the results of our enquiries into this growing threat with you.

Our 2011 survey shows that economic crime continues to be a serious issue affecting South African organisations. We hope that the information contained in this survey will assist readers in their ongoing endeavours to curb economic crime.

We would like to express our sincere appreciation to all those that agreed to participate in our survey as well as all the partners and staff that contributed their time and insights to this survey.

Louis Strydom
National Forensic Services Leader

Key findings

- We noted a steady decrease in the percentage of respondents that indicate they have experienced economic crime in South Africa since 2005.
- Globally reported incidents of economic crime have increased slightly since 2009 while South Africa has seen a decline during the same period.
- Cybercrime has emerged as a significant contributor to economic crime losses in South Africa and is now the fourth most common economic crime in South Africa and globally.
- Organisations in South Africa still have some way to go before optimal readiness for cybercrime is achieved.
- Respondents have reported decreases in the most common South African economic crimes of asset misappropriation and bribery & corruption.
- We have seen an alarming shift in the perpetrator profile towards senior management. This is also reflected in the types of economic crime that are being committed. Significant increases in tax fraud, market fraud (including price fixing) and insider trading were noted in 2011. These types of crimes typically require access to sensitive information and more sophisticated know-how which senior management possesses.
- Formal anti-fraud frameworks are becoming more effective at detecting economic crime. Organisations however need to re-visit their existing mechanisms to ensure they also cover the emerging economic crime threats.
- South African respondents report a significantly higher impact of non-financial consequences of economic crime than their global counterparts across all categories.

Introduction

Our 2011 survey addresses the various forms of economic crime and puts the spotlight on cybercrime.

This year 3,877 senior business representatives from 78 countries participated in our survey. Professor Peter Sommer and the London School of Economics assisted us with the scope, content and interpretation of survey data and the PwC Global Economic Crime survey continues to be the world's leading research programme into economic crime.

The 2011 survey results again show that economic crime remains a significant challenge for business leaders all over the world and specifically in South Africa - 60% of respondents in South Africa indicated that they had experienced some form of economic crime in the 12 months preceding the survey, compared to the global average of 34%.

We believe that the consistently higher figures presented for South Africa are indicative of a culture in which transgressions are reported and investigated.

Figure 1 – South African respondents subjected to economic crime over the last 12 months

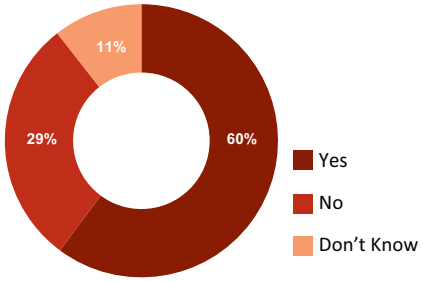
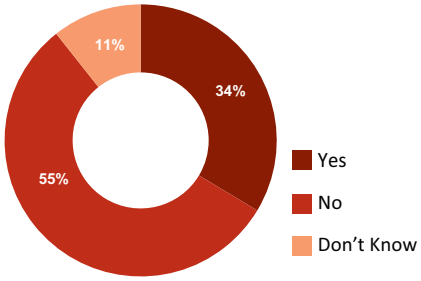


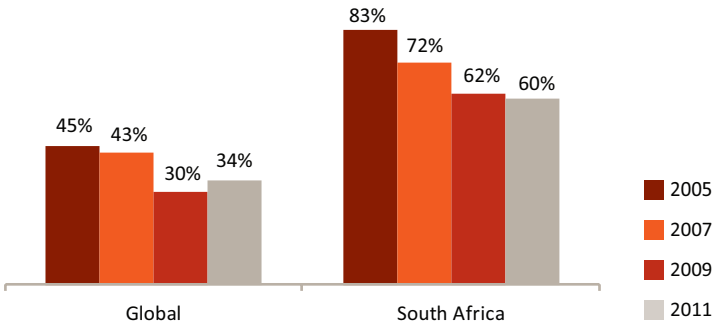
Figure 2 – Global respondents subjected to economic crime over the last 12 months



The prevalence of economic crime in South Africa has decreased a total of 23 percentage points since 2005. This is a significant decline.

The decrease in the overall incidence of economic crime in South Africa is as a result of corresponding decreases in the top 3 South African economic crime categories, namely asset misappropriation, bribery & corruption and financial statement fraud. However, it appears as though economic crimes that have traditionally not been as prevalent in South Africa, are on the increase. Formal anti-fraud frameworks are becoming more effective at fraud detection and organisations should revisit their existing anti-fraud frameworks to ensure that they can deal with the emerging threats as well as the 'traditional' threats.

Figure 3 – Trend of prevalence of economic crime since 2005



% respondents who experienced economic crime in the preceding 12 months (2011 and 2009) and in the preceding 2 years (2007 and 2005)

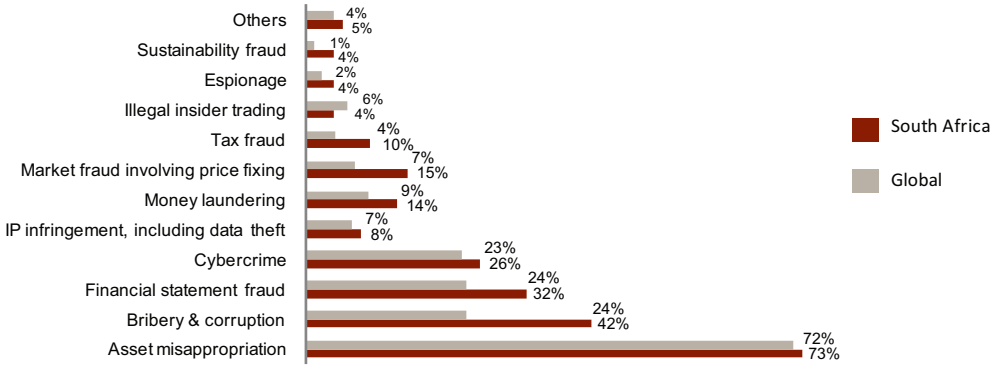
We analyse this overall position in the subsequent sections.

South African organisations reported significantly higher proportions of bribery & corruption, market fraud and financial statement fraud than their global counterparts in 2011.

Face of economic crime in South Africa

Figure 4 below depicts the incidence of the different types of economic crime globally and in South Africa. South Africa has a higher incidence in every category of economic crime except insider trading when compared to the global results. South African organisations report significantly higher levels of bribery & corruption, market fraud (including price fixing) and financial statement fraud than their global counterparts. Except for these crimes, the distribution of economic crime in South Africa mirrors the global picture.

Figure 4 – Types of economic crimes suffered in the 12 months preceding the survey



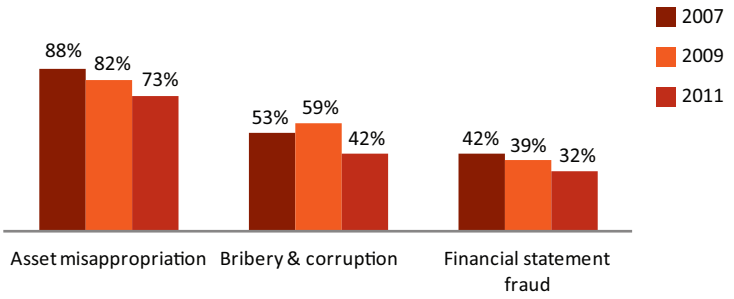
% respondents who experienced economic crime in the preceding 12 months

For the last six years asset misappropriation, bribery & corruption and financial statement fraud have been the top three economic crimes in South Africa. Figure 5 illustrates however that all three crimes have decreased during this period.

Asset misappropriation is once again the most prevalent category of economic crime in South Africa and globally. This is not surprising as asset misappropriation is among the easiest of economic crimes to detect as it involves theft of items with clear value.

In our previous surveys, when we asked respondents if they had experienced cybercrime, the response levels were very low and statistically insignificant. Hence, we combined the results with 'other types of fraud' in past survey reports. We focussed on cybercrime this year and reintroduced it in the types of fraud question as a separate crime category. It has emerged as one of the major economic crimes both globally and in South Africa with incidences of 23% and 26% respectively. The cybercrime phenomenon is explored in more detail in the next section.

Figure 5 – The big three



% South African respondents who experienced economic crime in the preceding 12 months (2011 and 2009) and the preceding 2 years (2007)

Figure 6 – Economic crimes that have shown significant increases in South Africa since 2009

% South African respondents who experienced economic crime in the preceding 12 months

As business transactions and social interactions move online, there is a clear shift from 'traditional' crimes to crimes involving the use of information technology.

Cybercrime in the spotlight

There is no standard globally accepted definition of cybercrime and this may make this phenomenon more difficult to analyse and counteract. PwC used the following definition of cybercrime in the GECS 2011 (formulated in conjunction with Professor Peter Sommer (survey academic partner)):

An economic offence committed using the computer and internet. Typical instances of cybercrime are the distribution of viruses, illegal downloads of media, phishing and pharming and theft of personal information such as bank account details. This excludes routine fraud whereby a computer has been used as a by product in order to create the fraud and only includes such economic crimes where computer, internet or use of electronic media and devices is the main element and not an incidental one.

Cybercrime does not leave the same physical traces as traditional crime and can be committed from remote locations. Due to these factors cybercriminals can operate with a level of anonymity and are able to conduct cross border activity without leaving their own homes.

Recently we have seen an increase in online activism often referred to as 'hacktivism'.

Groups like Anonymous.com are targeting organisations and governments whom they believe are behaving unethically or not in the best interest of the citizens they represent. The crimes committed by groups such as these are less focused on financial gain but are carried out to make a statement.

Motivations to conduct cybercrime can be diverse. However, financial gain remains a strong motivation to commit cybercrime and organised crime syndicates, for instance, are recruiting technologically skilled individuals to assist with their illegal activities.

The cost of breaches and the resulting investigations is causing South African organisations substantial losses that are difficult to absorb, however the damage to reputation after a breach can have a significant immediate impact and long term repercussions for organisations.

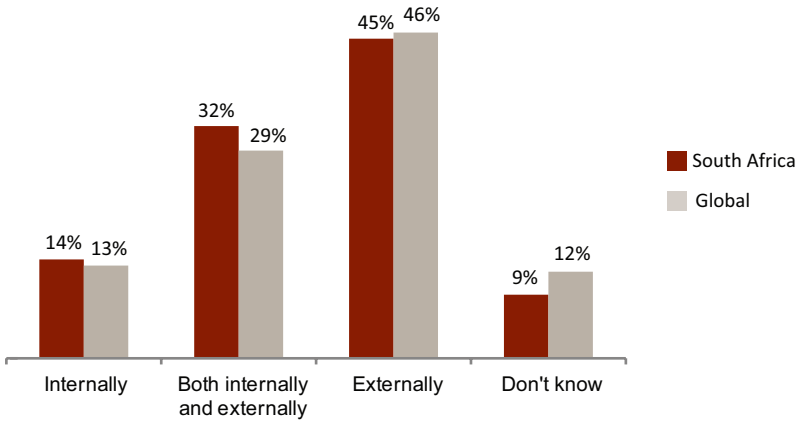
From a South African perspective new privacy legislation will be passed in the coming months and this legislation will impose fines on organisations that lose personal information. In addition to this organisations will also be required to disclose all breaches or loss of information to the regulator that will be appointed. This is a fundamental shift from how organisations previously dealt with such incidents as full disclosure can harm the reputation of organisations even if information was merely lost and not misused after a breach.

Increasing incidence of cybercrime in South Africa

Based on our survey, 60% of South African respondents felt the risk of cybercrime had increased in the last 12 months, compared to only 39% globally.

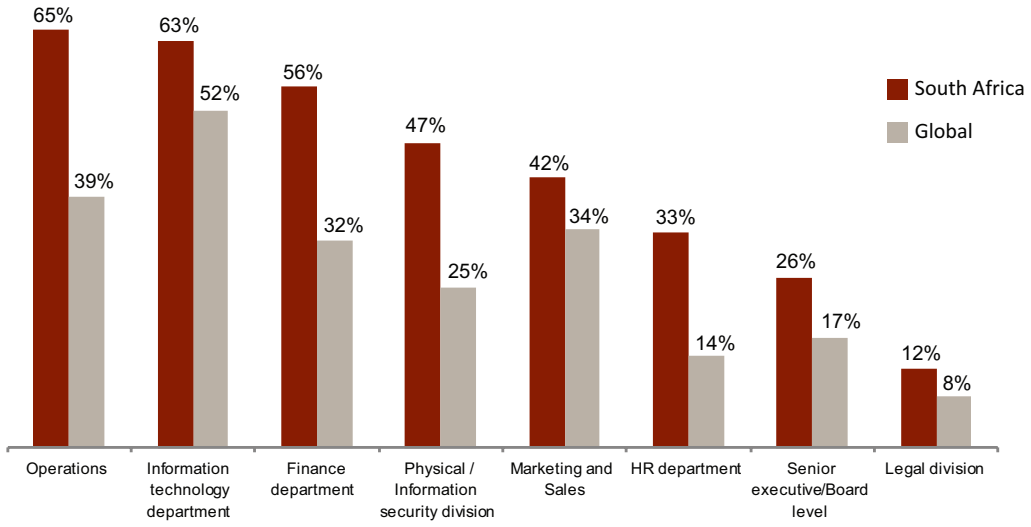
South African perceptions of the source of cybercrime mirror the international perceptions as illustrated by figure 7. It is worrying that about half of the respondents see cybercrime as only an external threat. Cybercrime requires access to protected information and employees, agents, contractors, customers and other individuals that have access to an organisation's premises and systems are likely to have access to such information. It is therefore important that organisations recognise the potential internal risks of cybercrime as well.

Figure 7 – Source of cybercrime threat - internal or external?



% of all respondents

Figure 8 – Internal sources about which South African respondents were very concerned



% of all respondents

Source of internal Cybercrime threat

Cybercrime threats could originate from various functions within an organisation. South African respondents view the most serious internal cybercrime threat as coming from Operations, Information Technology and Finance Departments.

South African respondents are also significantly more wary of Operations, Human Resource, Physical or Information Security and Finance divisions than their global counterparts.

Source of external Cybercrime threats

Figures 9 and 10 depict South African and global perceptions of the most likely origins of cybercrime threats (in alphabetical order). The reality is that cybercrime is a real global threat that can come from anywhere in the world, and is not restricted by jurisdictional boundaries like many other conventional crimes.

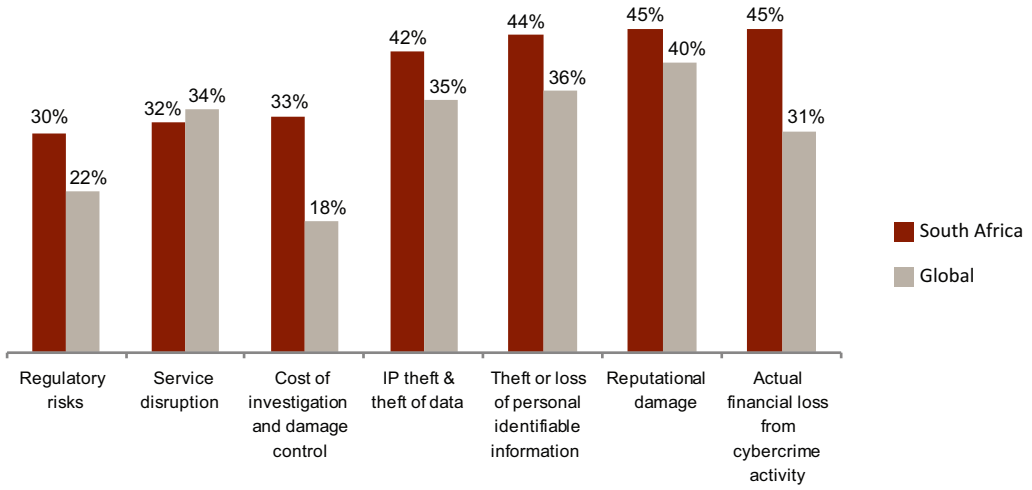
Figure 9: Global perception of the top 5 countries reported as the likely origins of cybercrime threats

Hong Kong (and China)
India
Nigeria
Russia
USA

Figure 10: South African perception of the top 5 countries reported as the likely origins of cybercrime threats

Hong Kong (and China)
Nigeria
South Africa
UK
USA

Figure 11 – Consequences about which respondents were 'very concerned'



% of all respondents

What concerns organisations?

We asked organisations what aspect of cybercrime they were very concerned about (figure 11). South African respondents indicated that reputational damage, direct financial loss and theft or loss of personal identifiable information are their main concerns. They are also much more concerned with the costs of investigations than the global respondents.

Cybercrime can cause more than just direct financial loss. Under the current proposed Protection of Private Information Bill, failures to secure clients' personal information will be punishable by fines and imprisonment.

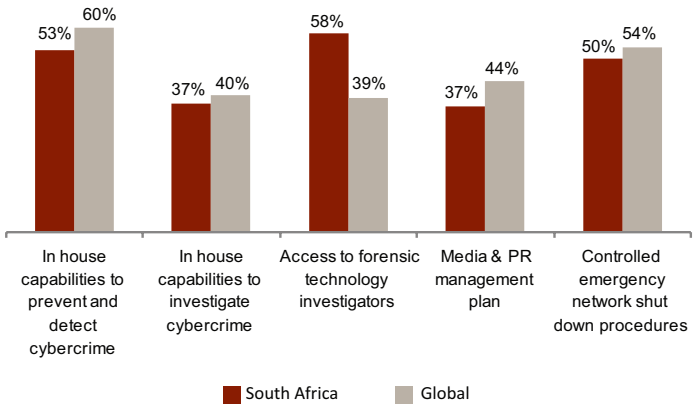
Readiness to deal with cybercrime

Figures 12 and 13 illustrate South African respondents' views on their organisation's readiness in relation to cybercrime.

Based on our survey, South African and global organisations still have a long way to go before optimal readiness is achieved:

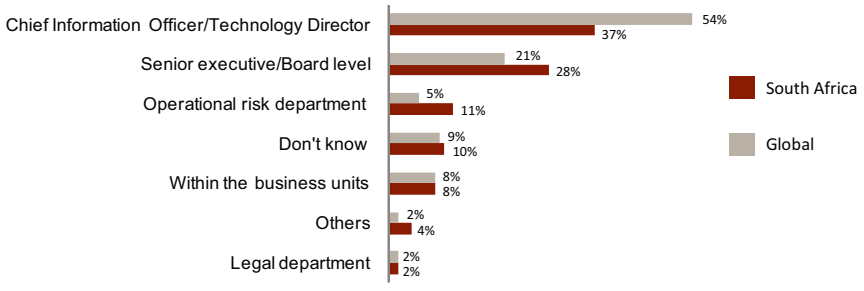
1. Figure 12 indicates that few organisations have all the elements of an holistic cybercrime prevention and response mechanism in place.

Figure 12 – Do you consider your organisation has adequate cybercrime incident response mechanisms/policies in place?



% of all respondents

Figure 13 – Where does the overall responsibility of preventing cybercrime risk reside within your organisation?



% of all respondents

Pre-emptive actions organisations should take to ensure readiness in the event of a cyber security attack

- Involve the CEO – the CEO and the Board need to be aware of cyber threats. They need to understand the risks and opportunities in the cyber world.
- Re-assess existing security measures and the preparedness of the organisation relating to cyber attacks. Unlike traditional economic crimes, cybercrime is fast paced with new risks emerging – organisations need to continually adapt their countermeasures to reflect these.
- Develop a response plan and create a response team (based on the assessed risks).
- Organisations that do not have specific resources available in-house should consult with external experts and include these in response teams.
- Awareness- individuals within organisations need to have a clear awareness of threats and response plans and measures.
- Educating all employees – an organisation needs to embed a "cyber aware" culture. Training to employees should be customised taking their respective roles and exposures into account.
- From an IT perspective, IT staff needs to be trained on how to deal with attacks in a manner that will not compromise the evidentiary value of the compromised systems.
- Take an active and transparent stance towards cybercrime – pursue perpetrators through legal means and communicate more publicly regarding actions the organisation is taking regarding the threats, incidents and responses.

2. One would expect that the overall responsibility to address the risk of cybercrime (or any other economic crime) lies with senior management. However, figure 13 shows that 10% of South African respondents did not know who should carry this responsibility. 28% believe the overall responsibility lies at the senior executive or board level while 37% place the overall responsibility on the Chief Information Officer (technology director). This is an interesting observation as Chapter 5 of the King III corporate governance report deals with IT and recommends that the board should be responsible for IT including IT security. The day to day execution of this responsibility can however be delegated to management and overseen by the board.

3. 42% of our respondents have indicated that either their board have never reviewed the risk of cybercrime or they do not know how often the board considers cybercrime. Many organisations are still getting to grips with the changes required by Chapter 5 of King III but we expect that senior management will be more involved in overseeing IT going forward. IT security should however not be viewed to be the sole responsibility of senior management. Divisional management must realise that the success of an organisation's information security strategy is also heavily dependent on proper execution across all divisions of an organisation.
4. 59% of respondents engage with external experts of cybercrime, but more than half of these stated their organisations only do so once an event has taken place. This approach is likely to lengthen the response time and make investigations less efficient, particularly if an organisation has a lengthy appointment process.
5. Given the relative increase in the prevalence of cybercrime, it is also surprising that 40% of South African respondents had not received cybercrime training or awareness communications of any kind during the preceding 12 months. The majority of global and South African respondents indicated that they considered human-based events such as workshops and presentations to be the most effective methods of cybercrime training and awareness creation. Computer based training was the second-most popular choice.

Social media

59% of respondents confirmed that their organisations monitor employees' usage of social networking sites. This is significantly higher than the global average of 40%. Online access is not as readily or cheaply available in South Africa as in developed countries and this may lead to a higher percentage of South Africans utilising their employer's internet access for personal use than their global counterparts. This could explain the propensity among South African organisations to monitor social media usage.

Despite the high degree of monitoring, only 18% of organisations that monitor social media usage have engaged with external experts to assist with developing policies in this regard.

Whilst social media sites such as Facebook, Twitter or LinkedIn may not be the real source of cybercrime, they can be used to social engineer cybercrime more effectively. For example, social media sites can be used to collect information about a targeted individual (also known as "spear fishing"), to research certain staff members or to install malware onto the user's computer, making the cybercrime more effective.

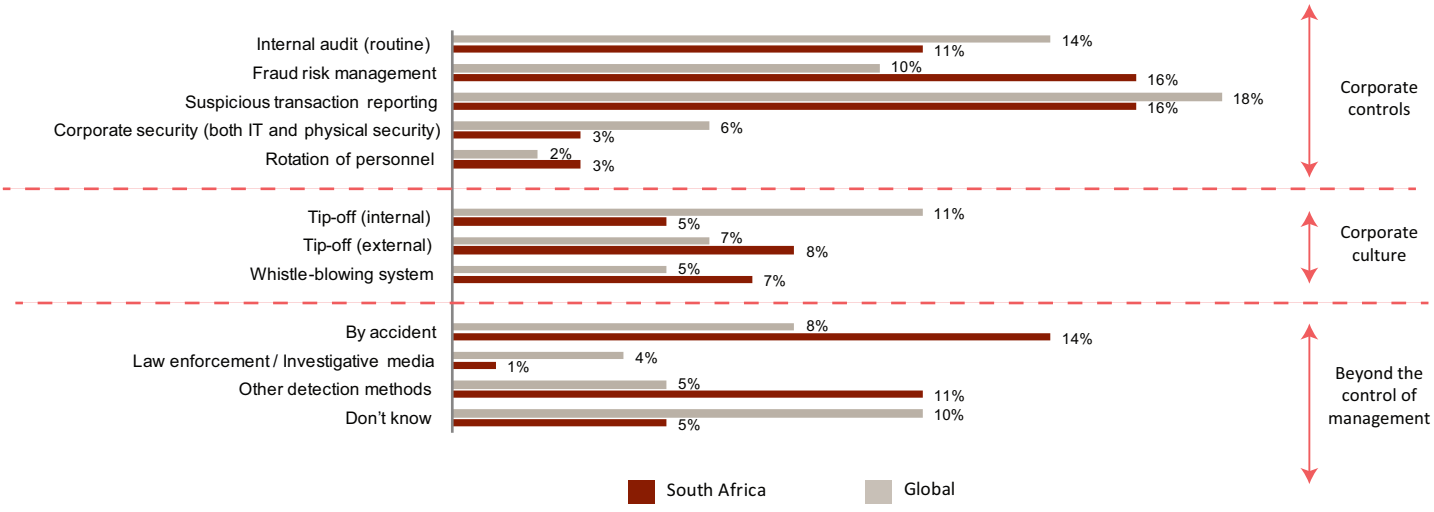
Are organisations detecting economic crime effectively?

Detection is a key element in managing the risk of economic crime. Detection methods should not be viewed in isolation – but as part of a comprehensive fraud risk structure.

Figure 14 illustrates that measures that management has control over (aggregate of corporate controls and corporate culture in figure 14 below), were responsible for 69% of the economic crime detections in South Africa (compared to 72% globally). However, 14% of detections occurred by accident which means there is room for improvement.

The most effective detection methods were formal fraud risk management procedures (including fraud risk assessments), automated suspicious transaction reporting (both contributed 16% of the detections) and internal audit (11%).The global statistics for these detection methods are illustrated in figure 14 below.

Figure 14 – Detection methods: Global and South Africa



% respondents who experienced economic crime in the preceding 12 months

The various tip-off methods (internal tip-off, external tip-off and formal whistle-blowing mechanisms) together contributed 20% to the economic crime detections, compared to 44% in 2009. These detection methods are so-called corporate culture measures and the significant decline in these methods may indicate that people are unwilling to report their colleagues and clients or business partners for committing crimes.

At the same time that tip-offs have declined, automated suspicious transaction reporting has increased. Automated suspicious transaction reporting is normally used to detect fraud in the financial services sector where sophisticated software tools are used to identify trigger conditions within the internal systems and thus draw the attention of management to potentially suspicious transactions. The contribution of automated suspicious transaction reporting has increased significantly since 2009, when it contributed only 3% of reported detections. It is possible that the reduction in head count in large organisations over the last few years has caused a relative reduction in human based detections. If so, does this mean that more economic crimes are going undetected due to reduced staff levels? Alternatively, it could mean that more organisations have chosen to implement automated detection tools for the first time and/or that the existing tools have matured.

Many organisations believe the formal whistle-blowing mechanisms to be a principal fraud detection method but it was responsible for only 7% of detections in South Africa.

Improving effectiveness of whistle-blowing mechanisms

The low detection rate of formal whistle-blowing mechanisms may be the result of the following factors:

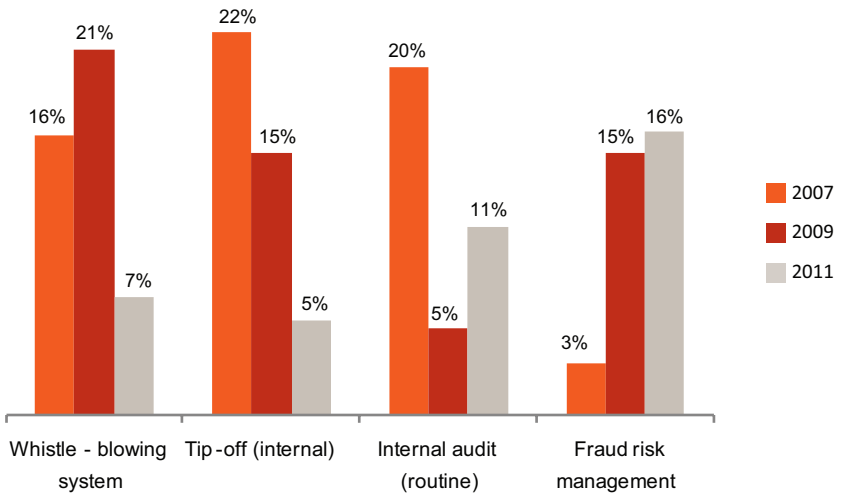
- Some companies may not have a formal whistle-blowing mechanism
- More awareness of available whistle-blowing channels may be required
- The importance of whistle-blowing may not be supported culturally within the organisation
- Employee's obligations to report misconduct may not be clearly communicated
- Organisations may need to do more to improve employee confidence in the whistle-blowing

Given the effectiveness of formal fraud risk management structures (which include fraud risk assessments), it is surprising that 28% of South African organisations had not performed a fraud risk assessment at all and 14% of respondents indicated that they were unsure whether any fraud risk assessment had been performed.

The most common reason given for not carrying out a fraud risk assessment was uncertainty about what a fraud risk assessment involves. A perception gap seems to exist regarding the value of fraud risk assessments. Our survey indicated that fraud risk management procedures (which include fraud risk assessments) were one of the most effective fraud detection methods, yet the second most common reason for opting against a fraud risk assessment was "perceived lack of value".

We analysed the trend in the effectiveness of the four main South African detection methods since 2007 in figure 15 below:

Figure 15 – Most effective detection methods in South Africa since 2007



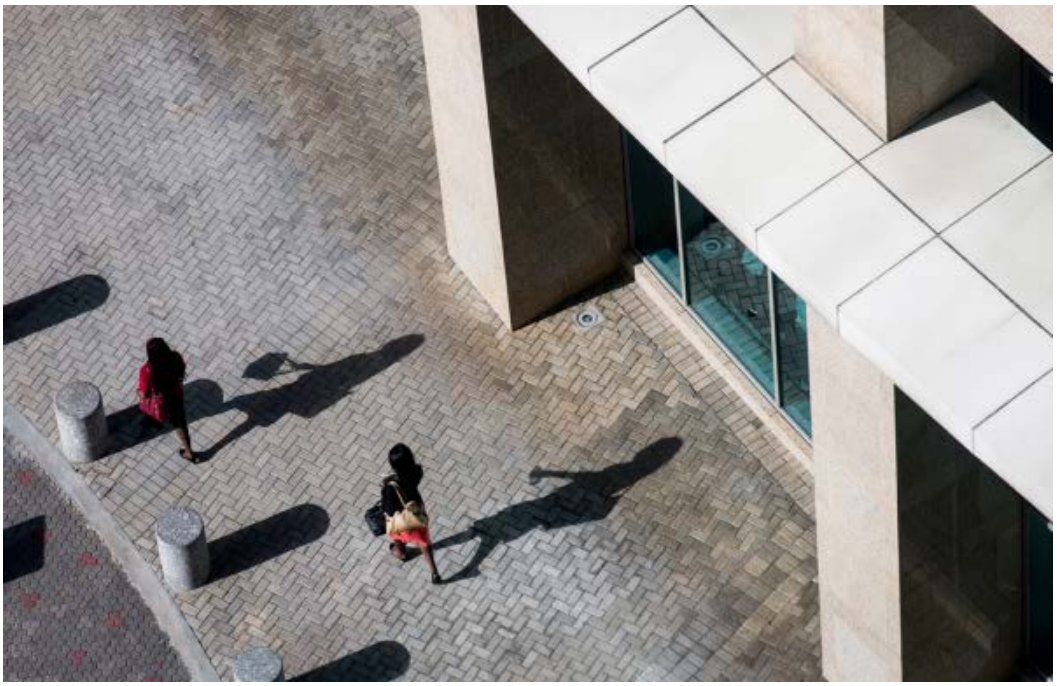
% South African respondents who experienced economic crime in the preceding 12 months (2011 and 2009) and the preceding 2 years (2007)

Fraud risk management is the only detection method that has become more effective from 2007 to 2011. Our experience has shown that formal fraud risk management measures are reaching greater levels of maturity in preventing and detecting economic crime in South Africa. The increase in economic crimes that have previously not been as prevalent in South Africa (figure 6) could suggest that organisations need to revisit their fraud risk management frameworks to ensure that they are able to deal with the emerging threats.

Internal audit had traditionally been one of the more effective detection methods, but dropped to 5% in 2009, though it has recovered to 11% in 2011.

Budget cuts during the financial downturn (2008 – 2009) may have played a role in the drop in the detection rate of internal audit to 5%. Our experience and discussions with internal audit executives indicate that internal audit spend was reduced during the height of the downturn but increased again in 2011. In addition, we believe that the increased focus on governance in South Africa contributed to increased internal audit detections as well.

Internationally, there has been a decline in the effectiveness of all detection methods, except automated suspicious transaction reporting.



A perception gap seems to exist regarding the value of fraud risk assessments.

47% of South African respondents stated that their losses for the 12 months before the survey amounted to more than US$ 100,000, with 11% reporting that their losses ranged between US$ 5 million and US$ 100 million. These losses are difficult to absorb in the current economic environment.

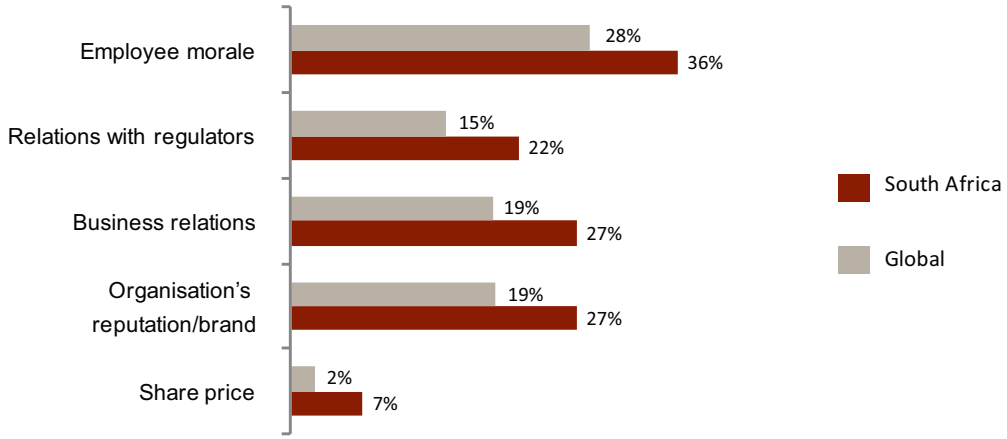
Costs of economic crime

Economic crime not only has a direct financial impact, but also non-financial consequences and organisations should not underestimate the harm of these non-financial consequences. South African respondents reported significantly higher impact in terms of collateral damage, than their global counterparts across all categories. This discrepancy relative to the global situation has also become more pronounced since our last survey.

Listed companies should note that the perception of a negative impact on share price is 3 times higher in South Africa than globally.

The negative impact on employee morale has been identified as the most significant non-financial consequence by South African respondents. The impact of this should not be underestimated. Experience has shown that negative employee morale can result in additional losses – it could embolden others within the company to commit attacks against the employer and contribute to poor performance.

Figure 16 – Percentage of respondents that stated that economic crime had 'significant impact' on the following areas (South Africa and Global)



% respondents who experienced economic crime in the preceding 12 months

Percentage of internal fraud committed by senior management in South Africa in 2011

36%

Percentage of internal fraud committed by senior management in South Africa in 2009

17%

Perpetrators and action taken

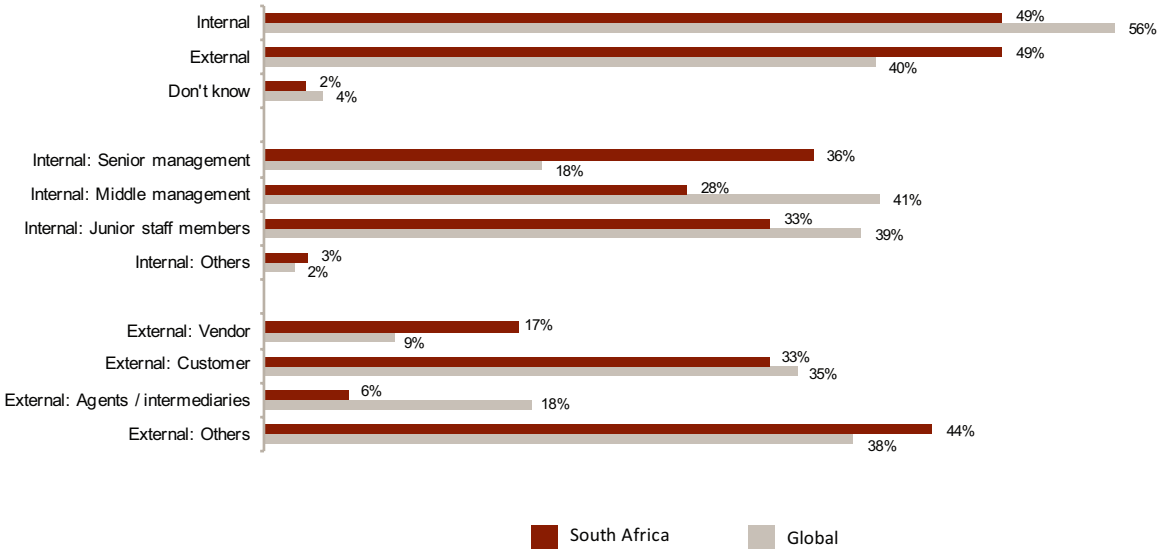
For the first time since our survey began, economic crime in South Africa is being committed equally by internal and external perpetrators. Globally the majority of crimes are still committed by internal parties.

Internally, we have seen an alarming shift in the perpetrator profile in South Africa towards senior management. In 2011, 36% of internal attacks were carried out by senior management compared to only 17% in 2009. This may also be reflected in the types of economic crime that are being committed.

Significant increases in tax fraud, market fraud (including price fixing) and insider trading were noted in 2011. These types of crimes typically require access to sensitive information and more sophisticated know-how, which senior management often possesses.

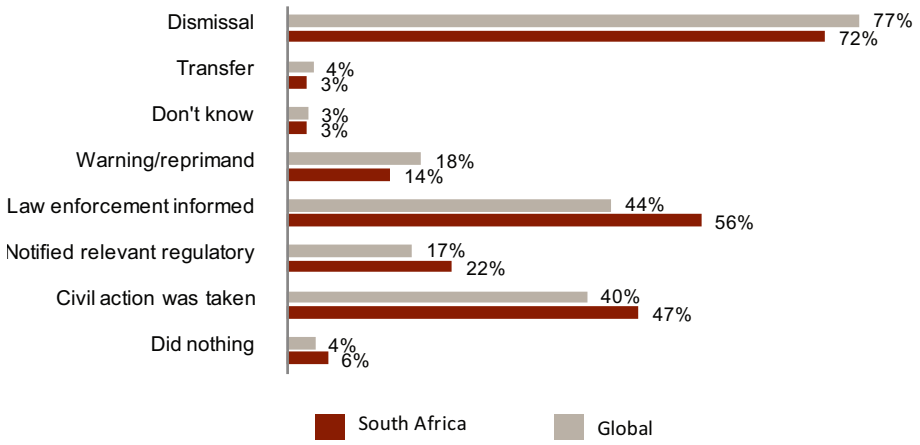
Conversely, fewer economic crime incidents are being committed by junior employees.

Figure 17 – Perpetrators of economic crime



% respondents who experienced economic crime in the preceding 12 months

Figure 18 – Action taken against internal perpetrators



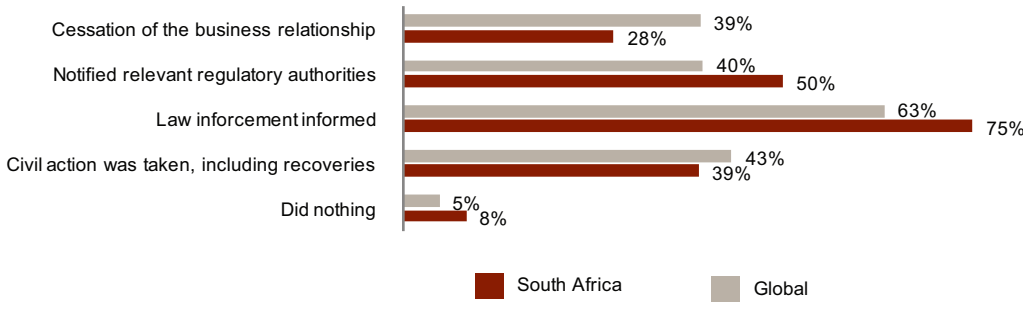
% respondents who experienced economic crime in the preceding 12 months

A slight decrease in the percentage of dismissals of internal perpetrators was noted since 2009. Overall South African organisations resorted to more stringent measures when dealing with internal perpetrators than their global counterparts (civil or criminal actions, and notifying regulatory authorities), but opted for dismissal in fewer instances than globally.

Interestingly, with regard to the most serious economic crime committed by insiders, South African entities took no action in 6% of cases, opted for transfers in 3% or warnings in 14% of cases. This is worrying as it suggests that these perpetrators still remain within the organisation and might be able to commit further transgressions. It is important for organisations to demonstrate 'zero tolerance' for economic crime and to set the right tone. Organisations should deal with fraudsters in an official and transparent manner, rather than dealing with them quietly and internally.

South African respondents were not as likely as their global counterparts to stop doing business with organisations whose employees were responsible for fraud attempts. Interestingly, South Africans were more likely to report external fraudsters to law enforcement, but less likely to take civil action, than their global counterparts.

Figure 19 – Action taken against external perpetrators



% respondents who experienced economic crime in the preceding 12 months

PwC Contacts

Louis Strydom
Gauteng
Johannesburg
+27 11 797 5465
louis.strydom@za.pwc.com

Charles De Chermont
Gauteng
Johannesburg
+27 11 797 5170
charles.de.chermont@za.pwc.com

Gerhard Geldenhuys
Central Region
Mafikeng
+27 18 386 4720
gerhard.geldenhuys@za.pwc.com

Colm Tonge
Gauteng
Johannesburg
+ 27 11 797 4007
colm.tonge@za.pwc.com

Horton Griffiths
Western Cape
Cape Town
+27 21 529 2067
horton.griffiths@za.pwc.com

Gerrit Jordaan
Namibia
Windhoek
+ 264 81 22 4246
gerrit.jordaan@na.pwc.com

Lionel Van Tonder
Gauteng
Pretoria
+27 12 429 0400
lionel.vantonder@za.pwc.com

Malcolm Campbell
Western Cape
Cape Town
+27 21 529 2676
malcolm.campbell@za.pwc.com

Peter Goss
Gauteng
Pretoria
+ 27 12 429 0331
peter.goss@za.pwc.com

Jacques Eybers
Eastern Cape
Port Elizabeth
+ 27 43 707 9802
jacques.eybers@za.pwc.com

Trevor Hills
Gauteng
Pretoria
+ 27 11 797 5526
trevor.hills@za.pwc.com

Trevor White
KwaZulu-Natal
Durban
+27 31 271 2020
trevor.white@za.pwc.com

South African Co-ordinator: Global Economic Crime Survey 2011

Freddy Fobian
Gauteng
Johannesburg
+27 11 797 4239
freddy.fobian@za.pwc.com

Further reading

PwC Global Economic Crime Survey 2011 – Global Edition
www.pwc.com/crimesurvey

PwC Global State of Information Security Survey 2012
http://www.pwc.com/gx/en/information-security-survey

The Cyber-savvy CEO
http://www.pwc.co.uk/eng/publications/delusions-of-safety-cyber-savvy-ceo.html

King's Counsel
Publication on the King III Report on corporate governance – including Chapter 5: Information Technology
http://www.pwc.co.za/en/king3/index.jhtml

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with close to 169,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

Designed by PwC Design Studio, South Africa (11-10149)

http://www.pwc.co.za/crimesurvey