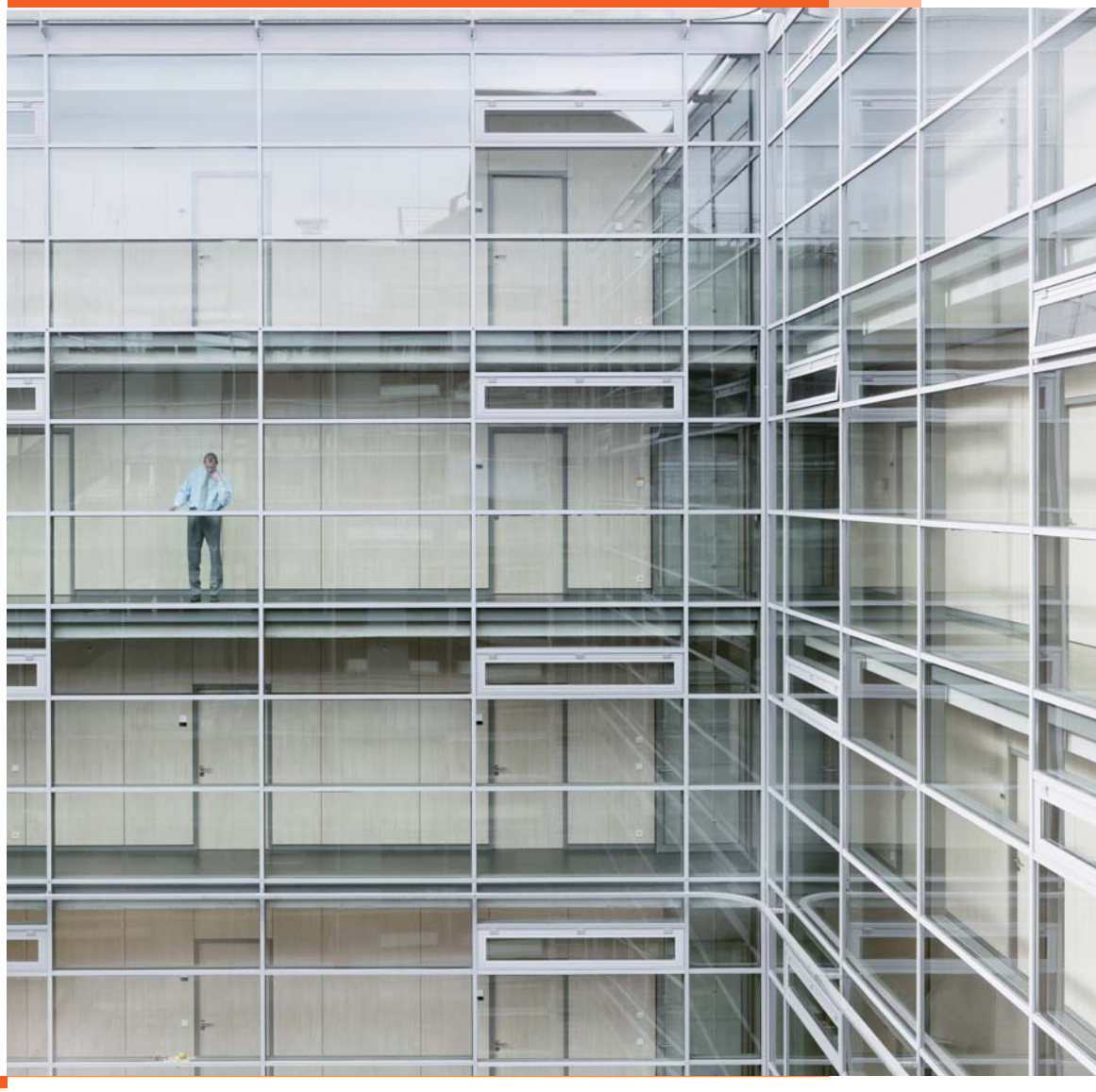
www.pwc.com/ke

A step ahead: Economic Crime in Kenya

Almost 4,000 organisations in 78 countries help provide a global picture of economic crimes.

November 2011



pwc

Contents

Introduction

Welcome to the 6th biennial Global Economic Crime Survey, the largest of its kind ever undertaken both globally and in Kenya. The survey reveals that against a backdrop of a global growth in economic crime, Kenya recorded the highest level of economic crime among all 78 countries surveyed with an incidence level of 66%, which is almost twice the global average of 34%. Kenya was placed second highest in 2009.

With almost 4,000 responses from senior executives in 78 countries, this is the most comprehensive survey of economic crime available to businesses globally, in Africa and in Kenya. It includes 91 respondents from Kenya, 123 from South Africa, 29 from Ghana and a few responses from several other African countries. The survey was conducted between July and October 2011 in conjunction with Professor Peter Sommer of the London School of Economics.

Kenya recorded the highest level of economic crime among all 78 countries surveyed with an incidence level of 66%, which is almost twice the global average of 34%

This summary report focuses on the results for Kenya based on the global survey. It seeks to understand and explore trends among economic crimes—including asset misappropriation, accounting fraud, bribery and corruption and cybercrime, among others—and the reasons behind them. It also aims to assess specifically the prevalence and effect of cybercrime on organisations, and how effectively organisations are dealing with the threat of cybercrime.

In this report, the responses from Kenya participants are compared with those for the rest of Africa and globally, and with the Kenya results from our 2009 survey. The 91 Kenyan responses from our 2011 survey came from senior representatives of large, medium and small organisations. Of these, 31% are listed companies, 46% are private companies and 22% are government/public sector organisations. Consequently the survey provides a useful indicator for evaluating economic crime and trends for Kenya both regionally and globally as well as the development of fraud trends over the last two years.

Asset misappropriation is the leading form of economic crime (both globally and in Kenya) having risen to a global incidence level of 72% and 73% in Kenya. Accounting fraud, which saw a big jump in our 2009 survey, remains the second most prevalent form of economic crime globally and in Kenya, although the incidence reported has fallen both among global and Kenya respondents. Incidences of money laundering appear to have increased across the board which suggests greater awareness of the crime. Other insights and comparisons are detailed below as well as in the global report at ***www.pwc.com/crimesurvey***

In this summary report we present the survey findings for Kenya including:

- the cost of economic crime,
- who is committing economic crime,
- what organisations are doing about it,
- how economic crime is detected, and
- perceptions of economic crime going forward.

We also focus on cybercrime in Kenya and how organisations can better safeguard themselves against this threat.

We would like to thank the organisations in Kenya that participated in the survey. Their responses indicate that economic crime is a rising threat to business requiring focused and continuous attention.

Economic crime in Kenya

The incidence of economic crime is rising in Kenya, in tandem with Africa and globally. A total of 66% of Kenyan respondents report having experienced at least one economic crime over the last 12 months, compared to 57% in 2009.

Kenya respondents now report the highest incidence of economic crime among all global respondents, at a level that is double the global average of 34% and seven percentage points above the Africa average of 59%. In 2009, Kenya ranked second globally with 57% of respondents reporting incidences of economic crime, compared to Africa (51%) and global respondents (30%).

From the above, it is clear that incidences of economic crime have risen significantly in Kenya and within Africa.

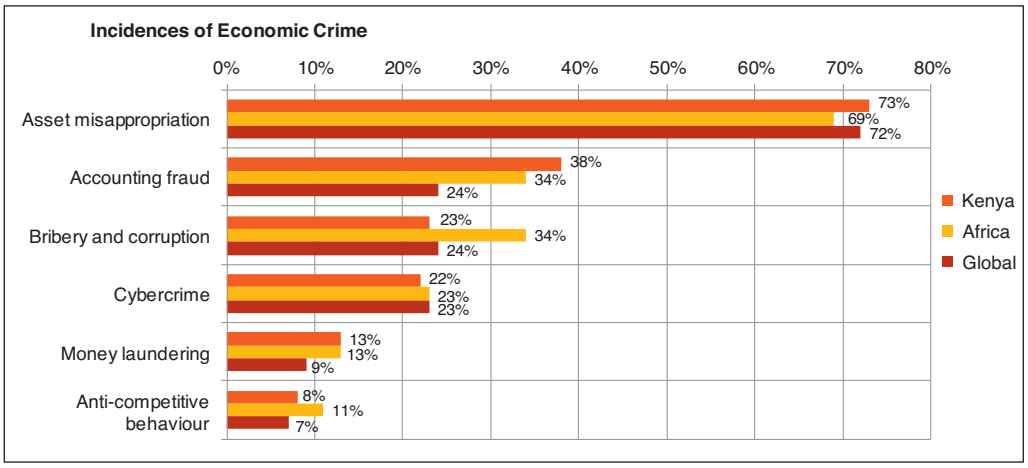
This could be due to a number of factors including increased public awareness of fraud since our 2009 survey, increased efforts to detect fraud, advances in technology and greater access to the internet leading to more ways of committing fraud.

Table 1

Territories that reported high levels of fraud (40% or more)	% respondents 2011	2009 comparison
Kenya	66%	57%
South Africa	60%	62%
Africa	57%	51%
UK	51%	43%
New Zealand	49%	42%
Spain	47%	34%
Australia	47%	40%
Argentina	45%	39%
France	45%	29%
USA	45%	35%
Malaysia	44%	28%

Among Kenyan respondents who reported having experienced economic crime over the last 12 months, 78% reported 1-10 incidences, a slight decrease from 2009 when 83% reported this level.

Figure 1



Among respondents in Kenya who reported incidences of economic crime, 73% named asset misappropriation as the most prevalent form compared to 57% in 2009. In Africa, 69% of respondents reported the same while globally 72% of respondents reported incidences of asset misappropriation. This indicates that asset misappropriation remains the leading economic crime globally. This could be due to the fact that asset misappropriation encompasses a wide range of economic crimes and fraud cases; many categories of fraud/ economic crimes could be classified as "asset misappropriation".

Asset misappropriation (including embezzlement and deception by employees) is defined as theft of organisation resources (including monetary assets/cash or supplies and equipment) by directors, others in fiduciary positions or an employee for their own benefit. Procurement fraud falls into this category, something that appears to be an area identified as being of heightened risk among Kenya respondents.

The number of respondents who reported accounting fraud has dropped significantly. In 2009, 63% of Kenya respondents reported incidences of accounting fraud, compared to 47% in Africa and 38% globally. In 2011, 38% of Kenya respondents reported accounting fraud, compared to 34% in Africa and 24% globally. This trend could be attributed to the global economic crisis resulting in a higher incidence of accounting fraud in 2009. Deficiencies in controls identified

This year's survey also focused on cybercrime which was not a category of economic crime in previous surveys

during the crisis may have been mitigated since then.

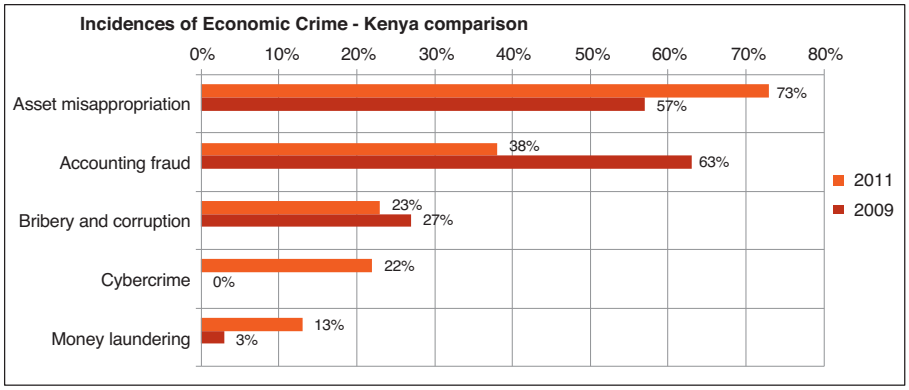
Bribery and corruption remains an issue especially in government related transactions although the prevalence has remained relatively unchanged in Kenya at 27%.

Money laundering has also increased significantly in Kenya with 13% of respondents reporting incidences over the last 12 months. In 2009, only 3% of respondents reported the same. This could be due to the anti-money laundering law passed in Kenya in the last 12 months and the consequent greater level of general awareness of the crime. Globally, money laundering incidences have decreased from 12% to 9%.

This year's survey also focused on cybercrime which was not a category of economic crime in previous surveys. This year's results indicate that cybercrime has become a key concern for organisations with 22% of respondents in Kenya reporting cybercrime and 23% of Africa and global respondents reporting the same.

The trends in the incidences of the different forms of economic crime in Kenya over the last two years are shown in the following chart:

Figure 2



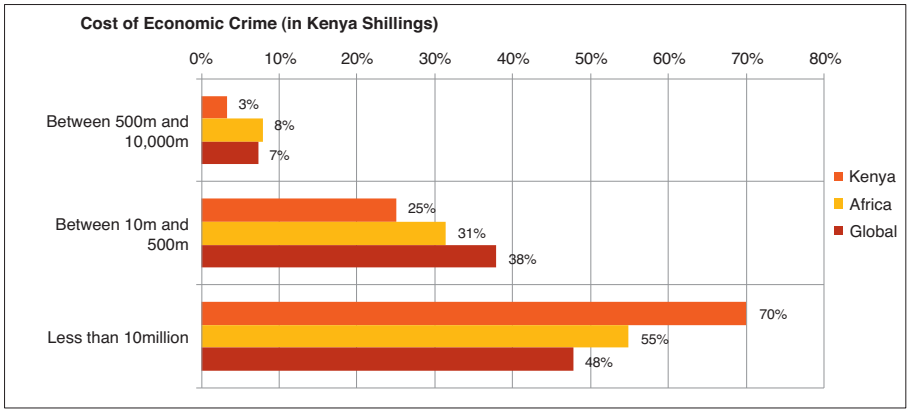
Cost of economic crime

Interestingly, the cost of economic crime does not appear to be rising. In 2011, 70% of respondents in Kenya reported that the cost of economic crime suffered was less than USD100k (around KShs 10m) compared to 57% in 2009. It also appears that economic crime does not have a significant impact on brand, share price, or business relations among most organisations.

Given the reported rising incidence level, it appears that more organisations in Kenya are experiencing economic crime but these crimes are costing less than in the past.

However, economic crime does appear to have an effect on employee morale according to 40% of Kenya respondents—a trend comparable to results among Africa and global respondents.

Figure 3



Who is committing the fraud and how do organisations deal with the perpetrators?

Most fraud is committed by internal fraudsters, according to 68% of Kenya respondents and compared to 59% in Africa and 56% globally. This follows the trend in 2009 where 70% of Kenyan respondents identified perpetrators as internal, with 68% in Africa and 53% globally stating the same. The most common perpetrators of fraud in Kenya are junior staff members (42%) and middle management (42%) which is a trend that is replicated globally.

Among external fraudsters, agents/ intermediaries lead the way in Kenya with 44% of respondents identifying this group as the perpetrators which differs significantly with the findings for Africa (17%) and globally (18%). In Africa and globally, most external fraudsters are customers (36% and 35% respectively). In addition, it was noted that most fraudsters are male (93%), between the ages of 31-40 years (46%), and have served the organisation between 3-5 years (42%). This is similar to the Africa and global results.

When dealing with internal fraudsters, most organisations prefer dismissing the perpetrator (81%) which mirrors the response across Africa (77%) and globally (77%). However, given the risks, it is somewhat concerning that 46% of Kenyan organisations chose to merely issue a warning to the perpetrator, something that could perhaps indicate a cavalier attitude towards economic crime. This also compares unfavourably with Africa (29%) and globally (18%). These findings suggest that organisations in Kenya may need to take a more serious approach to dealing with economic crimes so as to act as a deterrent against those considering such acts and to set the tone that fraud will not be tolerated at any level.

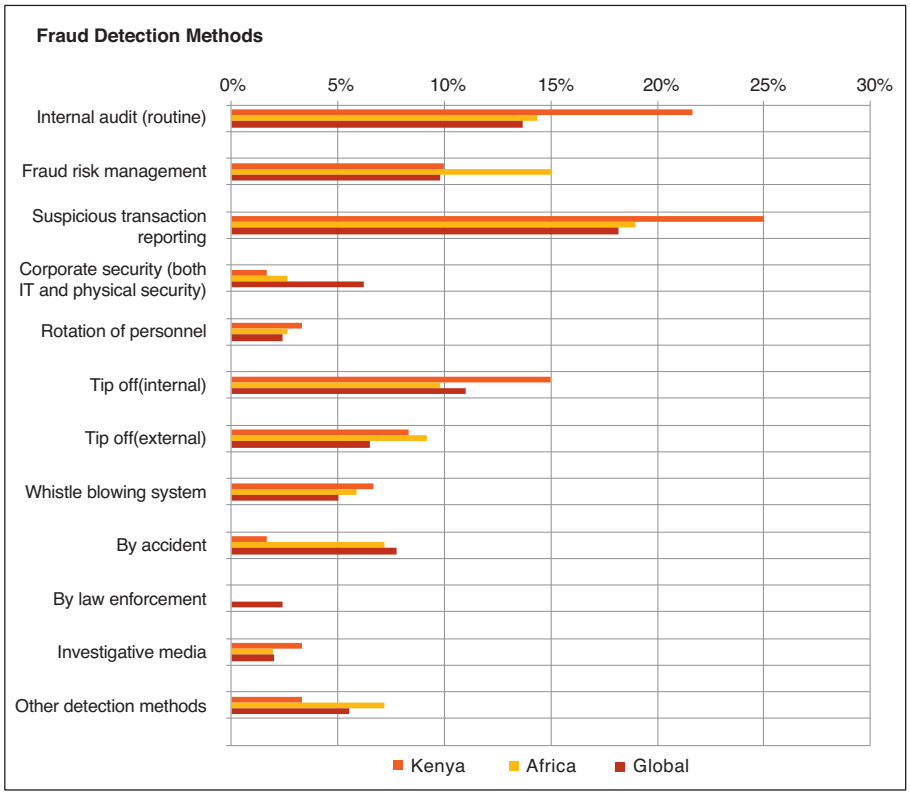
Most organisations in Kenya (61%) prefer to contact law enforcement when dealing with external fraudsters, similar to the results for Africa and globally. However, as with internal fraudsters, it is worrisome that 44% of organisations continue to maintain a business relationship with these fraudsters, which again raises questions about the seriousness of organisations' responses to economic crime.

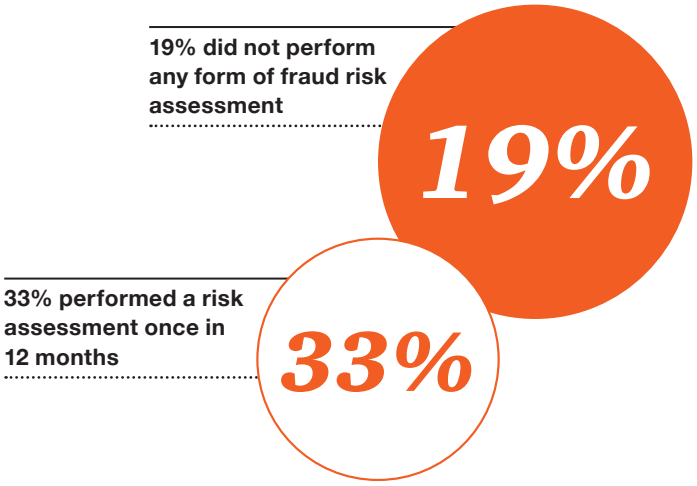
Detecting economic crime

The most effective methods of detecting economic crime are suspicious transaction reporting (25%) and internal audit (22%). This is also true among Africa respondents (19% and 14% respectively) and globally (18% and 14% respectively). In 2009, external tip-offs (27%) and internal audit (20%) were the leading methods of deducting economic crime in Kenya as well as in Africa and globally.

The graph below compares the different methods of fraud detection used by organisations in Kenya, Africa and globally.

Figure 4





As indicated in the table below most organisations in Kenya (more than 50%) believe that they will suffer some type of fraud in the next 12 months. Organisations in Kenya are therefore very pessimistic about the threat in the year ahead:-if anything however, they are insufficiently so, given the results for the last 12 months showing the incidence level of 66%.

Table 2

Type of economic crime	Likelihood of occurrence		
	Kenya	**Africa**	**Global**
Asset misappropriation	58%	51%	34%
Accounting fraud	41%	29%	14%
Bribery & corruption	44%	44%	27%
Cybercrime	36%	36%	26%
Money laundering	30%	22%	10%
Others	27%	46%	41%

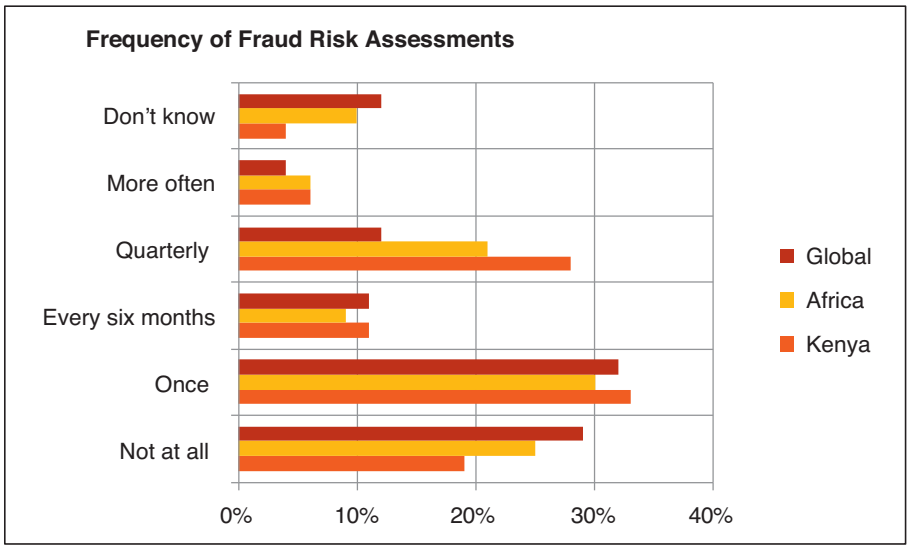
Despite the above statistics, 19% did not perform any form of fraud risk assessment, while 33% performed a risk assessment once in 12 months as shown below.

Most organisations in Kenya do not perform fraud risk assessments because, by their own admission, they do not know what an assessment entails (59%), while surprisingly some do not see the value in it (29%).

A total of 42% of Africa respondents and 30% globally do not know what a fraud risk assessment entails while 29% in Africa and 36% globally do not see the value in such assessments.

It seems that reactivity trumps pro-activity in this space; many respondents wait until after an incident occurs to engage an "expert".

Figure 5



Focus on Cybercrime in Kenya

Only 22% of Kenya respondents reported incidences of cybercrime

22%

This year's survey focused on the threat of cybercrime to organisations across the globe. For purposes of the survey, PwC defines cybercrime as:

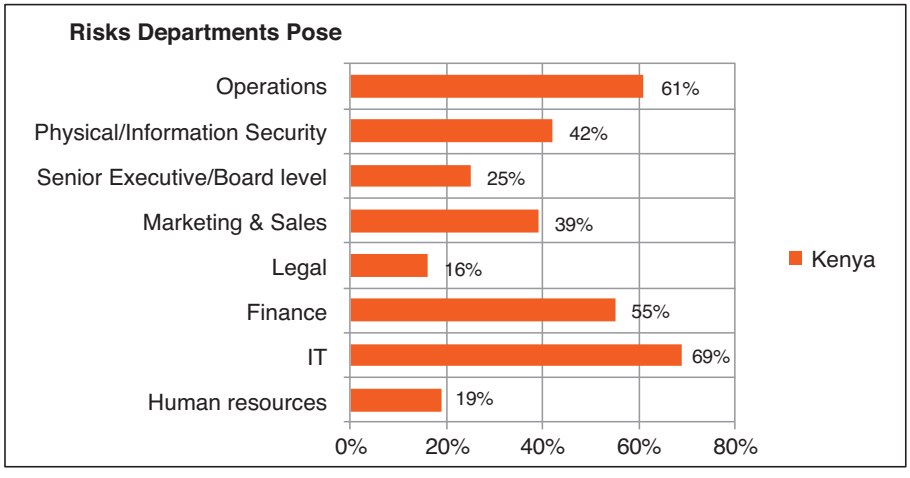
"Cybercrime, also known as computer crime, is an economic crime committed using computers and the internet. It includes distributing viruses, illegally downloading files, phishing and pharming, and stealing personal information like bank account details. It's only a cybercrime if a computer, or computers, and the internet play a central role in the crime, and not an incidental one."

Whilst only 22% of Kenya respondents reported incidences of cybercrime (which is close to the Africa and global averages of 23%), the perception of cybercrime is increasing rapidly in Kenya, as stated by 57% of respondents in Kenya (and 55% in Africa and 39% globally). This could be the result of greater media coverage as well as advances in technology.

Indeed, in Kenya most observers would agree that there has been a scaling up in media coverage of the threat posed by technology to organisations as well as of the actual incidence of frauds perpetrated using technology.

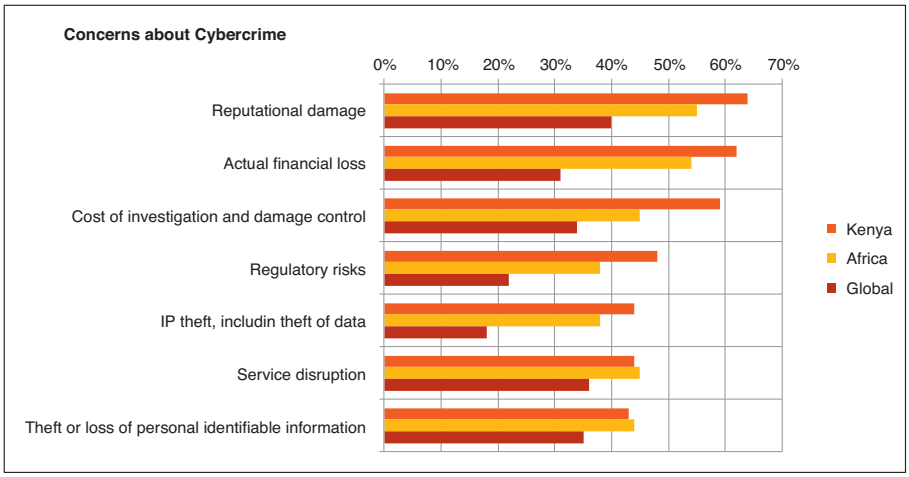
Most respondents see the threat coming from both internal and external sources (53%). IT, Finance and Information Security departments rank highly (69%, 55% and 42% respectively) in terms of the risk they pose to organisations as shown below.

Figure 6



A total of 51% of Kenyan respondents indicate that they have in-house capabilities to detect and prevent cybercrime, which is similar to the figure for Africa (52%) but this is below the global figure of 60%

Figure 7



A total of 51% of Kenyan respondents indicate that they have in-house capabilities to detect and prevent cybercrime, which is similar to the figure for Africa (52%) but this is below the global figure of 60%. Of more concern is the fact that only 35% of the Kenyan respondents indicate that they had the capabilities to investigate cybercrime should it occur. This is comparable to the Africa average of 36% and global average of 40%.

Among Kenya respondents, 45% (and 38% in Africa and 54% globally) indicate that overall responsibility for preventing cybercrime rested with the Chief Information Officer/Technology Officer/Chief Security Officer, implying that cybercrime is still viewed as an IT issue rather than a more organisation-wide issue. This is borne out by the fact that only 24% of respondents in Kenya (and 25% in Africa and 21% globally) indicate that overall responsibility rests with senior executives/Board members/C-suite. However, 31% of Kenyan respondents reported that the organisation's senior executives review the risks that cybercrime presents to the organisation on a quarterly basis. This is higher than the Africa average of 21% and global average of 11%, indicating that Kenyan senior executives have identified cybercrime as a priority and are being proactive in dealing with it compared to their African and global compatriots.

We believe that CEOs and C-suite level executives should understand the threats posed from the internet and take up the responsibility to prevent cybercrime in their organisations. Only after an incident occurs do half of respondents in Kenya consult an external expert, according to the survey, and 14% of Kenya respondents (19% in Africa and 15% globally) report that their senior executives do not consider cybercrime a risk at all, a worrying admission in light of recent incidents that have been covered in the media.

Forty-eight percent of Kenyan respondents (and 53% in Africa and 40% globally) report that their organisations monitor usage of social media (including Twitter & Facebook) by employees.

A total of 87% in Kenya and similar percentages in Africa and globally report that their organisations monitor internal or external electronic traffic, including web-based traffic, to combat the risks of social media and networking, while 64% (and 60% in Africa and 62% globally) report that employee contracts refer to proper use of internal documentation and information.

This shows an awareness of the risks posed by social media and it is encouraging to note that most organisations have taken steps to deal with these risks.

Meanwhile, 47% of Kenya respondents (and 43% in Africa and 40% globally) report having seen an e-mail announcement, poster and/or banner regarding cyber security. However, 31% of respondents reported that they had not received any form of training related to cyber security. Whilst this is an area for concern, it is comparable to the Africa average of 36% and global average of 42%, as shown below.

Table 3

Type of training	Kenya	Africa	Global
Email announcements/posters/banners	47%	43%	40%
Human-based events (Presentations/team meetings/workshops)	35%	28%	25%
Computer based training	24%	21%	22%
None	31%	36%	42%

31% of respondents reported that they had not received any form of training related to cyber security

What can organisations do to defend themselves against cyber security attacks?

The picture is decidedly mixed for organisations in Kenya facing cybercrime. There are several ways that organisations can build awareness and address this threat:

- **Clarify roles and responsibilities –** CEOs need to come to grips with internet threats—which is why PwC has introduced the concept of the 'cyber savvy CEO'. We believe that leadership by a cyber savvy CEO will enable the organisation to understand the opportunities and realise them securely and sustainably through effective security. Those who truly understand the risks and opportunities of the cyber world will effectively differentiate and protect themselves going forward.
- **Re-assess the security function and preparedness of the organisation should a cybercrime occur –** Organisations already have IT security functions that may be doing a good job in protecting against traditional threats. But as new risks emerge, the focus needs to be on upgrading or transforming existing capabilities to ensure that their security strategies fully encompass cyber security.
- **Awareness –** To align their security functions and priorities as closely as possible with the realities of the cyber world, organisations need a clear understanding of the current and emerging cyber environment. This demands situational awareness, which is a prerequisite for well-informed decisions on cyber security actions and processes.
- **Create a cyber incident response team –** Traditional organisational structures may have the unintended effect of delaying the quick and decisive responses needed in the cyber environment. Many organisations will already have an incident response team but the speed and unpredictability of cyber threats mean that it may need to be adapted and streamlined. A well-functioning cyber incident response team means an incident spotted anywhere in the business will be tracked, risk-assessed and escalated.
- **Educate all employees –** An organisation needs to embed a 'cyber awareness' culture by recruiting those with the relevant skills so that this knowledge can be shared with all employees and creating a 'cyber-aware' organisation which is better able to protect itself. Some organisations may even want to consider more radical approaches, such as putting younger employees on a board committee focused on cyber security.
- **Take a more active and transparent stance towards cybercrime–** The unpredictable and high-profile nature of cyber threats tends to engender a defensive mindset. But a number of cyber-savvy organisations are now getting ahead of this threat by adopting a more active stance towards attackers, pursuing them more actively through legal means and communicating more publicly about their cyber threats, incidents and responses. By taking a more active stance, the organisation can show that it takes attacks seriously and will strive to bring offenders to justice.

Concluding remarks

Organisations need to be more proactive in identifying, preventing and detecting fraud

There are some positive signs with regard to economic crime in Kenya. Accounting fraud has reduced significantly, organisations are increasingly aware of the threat of cybercrime, and are getting better at detecting money laundering, thanks to new legislation and improved awareness.

Notwithstanding the above, there are some sobering results for organisations in Kenya. Economic crime in Kenya and globally is on the rise. Kenyan firms report double the global average incidence of economic crime.

As a result there is an increasing need to remain vigilant, particularly in relation to asset misappropriation and cybercrime. Organisations also need to be stronger in dealing with perpetrators of economic crime so as to deter others. This applies to both internal and external perpetrators.

Fraudsters are getting more sophisticated, especially with advances in technology.

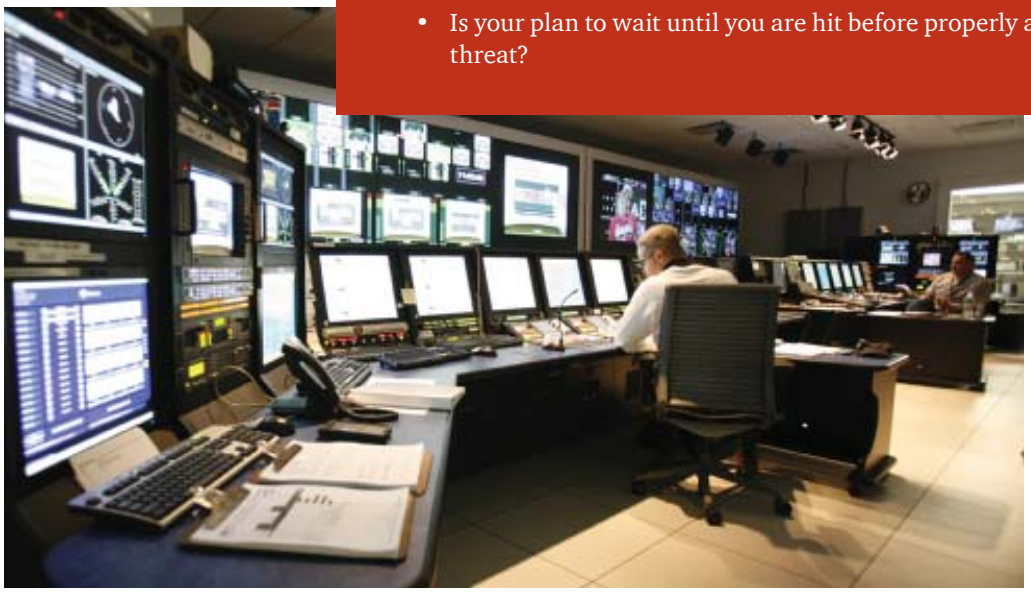
Consequently, organisations need to be more proactive in identifying, preventing and detecting fraud. This can be done by:

- setting the right tone at the top i.e. dealing effectively with fraudsters;
- having savvy IT and cyber security teams that are adequately trained to deal with threats; and
- carrying out periodic fraud risk assessments.

The good news is that organisations that are proactive identify risks and detect incidences of economic crime early enough before significant damage can be done. Moreover, for those with limited resources or experience, there is a great deal of local professional expertise to help in this fight.

Five key questions all organisations should ask themselves

1. ***Do you really show the right tone at the top in dealing with economic crime?***
   - Or do you merely pay lip service as required?
   - Do you practice zero tolerance?
   - Is senior management even aware of major incidences of economic crime in your organisation and the resulting cost?
2. ***How do you deal with fraudsters when you uncover wrongdoing?***
   - If they are employees - do you merely let them off with a warning ?
   - If they are external parties – agents or customers say – do you just continue business as usual?
3. ***How sure are you of the robustness of your procurement processes?***
   - Are you confident that you are getting value for money and competitive terms?
   - How often do you take an independent look at your controls around the procurement cycle?
4. ***Is your CEO or organisation head truly "cyber savvy" and is your organisation able to detect and investigate cybercrime?***
   - If not is leadership seeking to get trained and up to speed as a priority?
   - Is leadership putting in place a cyber awareness culture?
5. ***Does your organisation undertake regular fraud risk assessments? If not,***
   - Is this because you do not see the benefit?
   - If it is due to the perceived cost in recruiting staff or engaging outside professionals, how do you reconcile this with the likely cost of economic crime?
   - Is your plan to wait until you are hit before properly addressing this threat?



Contact us

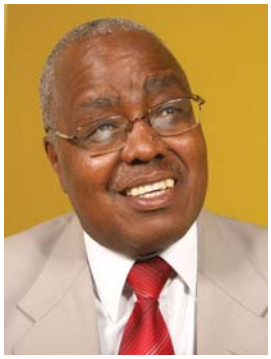
At PwC, we can carry out fraud risk assessments and cyber security reviews to help you identify key risks and threats. Our assessments are fast and cost-effective, combining global leading best practices and in-market experience. In addition, we provide investigation services to detect economic crime and determine how it was committed and who is responsible. Our regional team of dedicated specialists has conducted some of the most complex and high profile investigations undertaken in Kenya and regionally in recent years.

Martin Whitehead
Partner
Forensic Services
martin.whitehead@ke.pwc.com

Martin Whitehead is a partner heading up the firm's regional Investigation and Forensic Services practice.

He has more than 20 years of experience in providing clients with advice covering forensic services, financial restructuring, asset recovery and anti-corruption initiatives.

He is a chartered accountant with an MBA from INSEAD and a masters degree in management from Stanford Graduate School of Business.



Alphan Njeru
Partner
Head of Public Sector Group
alphan.njeri@ke.pwc.com

Alphan Njeru leads the Public Sector Group in Kenya and the Africa Central network of firms. This group is involved in providing Advisory and Assurance services to Governments, Development Partners and Non-Government organisations within the region. He has been with the firm for over 32 years during which he has been involved in Assurance and Advisory related type of work.

Alphan is a recognised public sector practitioner and his views and opinions are sought for from both within the firm and outside on matters of governments' policy, implementation and interpretation.

Patrick Matu
Manager
Forensic Services
patrick.matu@ke.pwc.com

Lucy Munga
Senior Manager
Cyber Security
lucy.munga@ke.pwc.com

For more information, visit our website www.pwc.com/ke

www.pwc.com/crimesurvey

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.