Economic crime: a threat to business processes

52% One in two respondents reported experiencing economic crime in the last two years

36% More than one in three respondents reported being asked to pay a bribe to get business

54% More than half of reported economic crimes were committed by middle management
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 Foreword</td>
</tr>
<tr>
<td>4 Introduction</td>
</tr>
<tr>
<td>5 Economic crime in Kenya</td>
</tr>
<tr>
<td>5 What is happening? Respondents reported a decline in incidences of economic crime</td>
</tr>
<tr>
<td>7 Cost of economic crimes</td>
</tr>
<tr>
<td>9 Shift from the “big three” to “big five”</td>
</tr>
<tr>
<td>9 Asset misappropriation</td>
</tr>
<tr>
<td>9 Accounting fraud</td>
</tr>
<tr>
<td>10 Bribery and corruption</td>
</tr>
<tr>
<td>10 Procurement fraud</td>
</tr>
<tr>
<td>10 Cybercrime</td>
</tr>
<tr>
<td>11 Who is doing it? And how are they dealt with?</td>
</tr>
<tr>
<td>11 Internal fraudster</td>
</tr>
<tr>
<td>11 External fraudster</td>
</tr>
<tr>
<td>12 Actions taken against perpetrators</td>
</tr>
<tr>
<td>12 Profile of a typical fraudster</td>
</tr>
<tr>
<td>13 The enemy hiding in plain sight</td>
</tr>
<tr>
<td>13 To catch a thief</td>
</tr>
<tr>
<td>15 Fraud risk assessments and cybercrime</td>
</tr>
<tr>
<td>15 Fraud risk assessments</td>
</tr>
<tr>
<td>17 Cybercrime</td>
</tr>
<tr>
<td>20 Perception of corruption, money laundering and competition</td>
</tr>
<tr>
<td>22 Bribery and corruption – the Global perspective</td>
</tr>
<tr>
<td>23 Conclusions</td>
</tr>
<tr>
<td>24 Methodology</td>
</tr>
<tr>
<td>25 Terminology</td>
</tr>
</tbody>
</table>
It has been two years since we last conducted our Global Economic Crime Survey. In 2011, a high percentage of our Kenyan respondents reported having suffered an incidence of economic crime - two out of every three of our respondents! These results came at a time of consumer price inflation, high interest rates and wildly fluctuating exchange rates.

Since then, most of these indicators have stabilised and Kenya has experienced considerable political and economic change. The peaceful conclusion of elections, the move to devolved government and major changes in tax legislation have all had an impact on organisations and the economy. Continued technological advancements have changed the lives of millions of Kenyans.

How has economic crime changed against this backdrop of political, economic and social developments? This year’s results show a reduction in the reported incidence of economic crime compared to the 2011 survey results. However, there is still cause for concern because Kenyan respondents continue to report relatively high rates of economic crime compared to other countries surveyed globally. Furthermore, for the 52% of respondents in Kenya who reported experiencing economic crime in the last 24 months, the frequency of incidences has tended to increase and the cost impact tends to be greater.

Not only has the incidence rate of economic crime changed, so has the nature of economic crime reported. Along with Asset Misappropriation, Accounting Fraud and Bribery and Corruption, our survey results reveal high levels of Cybercrime and Procurement Fraud. This shows that the threats and trends of economic crime are constantly evolving, particularly with the increased use of technology and technology-enabled processes across organisations.

We are also concerned that the frequency of Fraud Risk Assessments in Kenyan organisations has reduced since our last survey, and that 39% of respondents do not know what a Fraud Risk Assessment entails. Contributing factors could include a lack of sufficient knowledge and a poor understanding of the importance of proactive fraud risk management, cost-cuts and/or a reactive culture of dealing with fraud risks. We believe the changing trends and threats of economic crimes call for a serious rethink.

Combating economic crime requires the attention of all key organs within an organisation, not just the Internal Audit or Risk and Compliance functions. Throughout this report, we draw a number of parallels to our recent Africa CEO Survey and specifically the results of our CEO Survey in Kenya, which were published in PwC’s 3rd annual Africa Business Agenda (2013). One trend from the CEO Survey that concerns me is that CEOs in Kenya are almost evenly split with regard to whether accountability for risk management responsibility is centralised (45%) or decentralised (55%) within their organisations. Our Global Economic Crime report investigates this further and shows that effective risk management must be implemented holistically across an organisation to combat economic crime effectively. Everyone has a responsibility for combating economic crime.

This report provides a number of practical steps to combat economic crime which include, at a minimum, adopting the mind-set of “a state of compromise” (the point of view that internal systems have already been breached), identifying critical assets and recognising the vulnerabilities of your organisation.

This report also helps to highlight a number of relevant questions for organisations like yours, such as: How can organisations in Kenya manage the changing face of economic crime? How can they effectively detect and deter cyber attacks? Are procurement processes robust enough to ensure the integrity of procurement? Are organisational controls strong enough to mitigate the risk of asset misappropriation? Is there a no-tolerance culture to bribery and corruption? Is the management team incentivised to report accurate results? And above all, if an economic crime has occurred, will it be detected in a timely manner and do you have an appropriate response mechanism?

The real story in this report is not so much that economic crime stubbornly persists. The real story is that economic crime is threatening business processes, eroding the integrity of employees and tarnishing reputations. That is why our 2014 report focuses on how and where it may be affecting organisations so they can address the issue from a preventive and strategic perspective.

In this report, we summarise the Kenyan experience of economic crime since 2011, who is committing it and how it is detected. We hope the trends we have identified will assist you in identifying the vulnerabilities in your organisation and we would look forward to discussing with you how best to address the threat of economic crime. We take this opportunity to thank the organisations and individuals in Kenya that participated in the 2014 PwC Global Economic Crime Survey.
In instances of economic crime, Kenya is still above the Africa average of 50% and substantially higher than the global average of 37%.

**Introduction**

We are pleased to present our seventh biennial Global Economic Crime Survey report and third biennial Kenya report which aims to give you insight on corporate attitudes towards economic crime as well as seek to understand and explore the trends and motives behind it.

Economic crime is a global phenomenon that cuts across all regions, industries and organizations. In our 2014 survey we received over 5,000 responses from senior executives in 99 countries making this survey the largest in its category globally and in Kenya. The number of respondents from Kenya has steadily increased with every survey. In 2014 there were 124 respondents compared to 91 in 2011 and 53 in 2009. Respondents from Kenya accounted for 21% of Africa survey respondents and 53% for East Africa region. These respondents consist of senior executives and representatives from large and medium sized organisations. The majority of these respondents were from the Audit and Finance departments.

In the past, the most predominant forms of economic crime have been asset misappropriation, accounting fraud and bribery and corruption, typically referred to as the “big three”.

In recent times and as revealed by this survey, procurement fraud and cybercrime are now highlighted as additional prevailing economic crimes, shifting from ‘big three’ to ‘big five’. This shift is in line with global survey results, although asset misappropriation is still the leading form of economic crime in Kenya with a high incidence level of 77%, followed by accounting fraud at 38%. Procurement and cybercrime have prominently featured at incidents levels of 31% and 22% respectively. An interpretation of these results indicates a need for more vigilance in the business processes affected by these additional forms of crime.

This year’s survey also drew a distinction between economic crimes of a “systemic” nature, such as bribery and corruption, money laundering, and anti-competitive practices. These are regularly examined by regulators and represent a greater risk than “episodic” frauds (such as asset misappropriation or accounting fraud, which occur as the result of a specific situation/ set of circumstances). One thing that is becoming increasingly clear is that economic crime at its worst takes advantage of the tension within a business between the struggle for profits versus the struggle for compliance.

A more detailed description of the ‘big five’ will be explored in subsequent sections of this report and the global report is available at [www.pwc.com/ke/crime-survey](http://www.pwc.com/ke/crime-survey)
Despite fewer respondents being affected by economic crime …those affected experienced it more frequently.

**Economic crime in Kenya**

What is happening? Respondents reported a decline in incidences of economic crime

The proportion of Kenyan respondents who experienced economic crime since the last survey in 2011 has reduced. 52% of Kenyan respondents in the current survey reported having experienced some form of economic crime, versus the previous survey in 2011 where the incidence was higher at 66% of respondents in their organisations. This decline could be attributed to more aggressive efforts and deliberate actions by organisations to address the problem. Having been in the upper quartile in recent years, in 2014 South Africa topped the list of countries surveyed with 69% of respondents reporting that they had experienced economic crime compared to 60% in 2011.

Technological transformations, including the increasing digitization of personal data and processes, as well as cloud, are enabling more and more harmful incidents of economic crime.

In Kenya, technological transformation has largely been driven through the use of mobile telephones and smart phones. We have seen an increasing appreciation by organisations of their vulnerability to economic crime. Their exposure to economic crime increases as they trade more and rely on third parties for various transactions such as debit cards, online trading and mobile money transactions.

In spite of this notable decrease in instances of economic crime, Kenya is still above the Africa average of 50% and substantially higher than the global average of 37%. Kenyan organisations still need to place more emphasis and dedicate resources to tackle the high instances of economic crime.
Despite a decrease in the incidence of economic crime, the survey data shows that for those organisations that reported suffering economic crime, the frequency of incidents has increased since 2011. There was a 107% increase in the relative number of responses reporting between 11-100 incidences of economic crime over a 2 year period, while those reporting fewer than 10 incidents during this period reduced from 78% to 63%, a 24% decrease. Thus, despite fewer respondents being affected by economic crime in 2014, those that were affected experienced it more frequently. This may indicate:

- particular industries being more susceptible to economic crime than others
- the impact of technology on businesses
- the need for organisations to operate in a global market
- inadequate and insufficient knowledge/capacity within an organisation to deal with fraud and related economic crimes

The table below summarises the survey responses on the number of incidents suffered by those respondents who reported having experienced some form of economic crime over a 2 year period to October 2013.

<table>
<thead>
<tr>
<th>Number of Incidents Suffered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less then 10</td>
</tr>
<tr>
<td>2014 Kenya</td>
</tr>
<tr>
<td>2014 Africa</td>
</tr>
<tr>
<td>2014 Global</td>
</tr>
<tr>
<td>2011 Kenya</td>
</tr>
</tbody>
</table>

Although this is largely in line with the global trend, in Kenya it would appear that organisations are consistently under threat of economic crimes with the number of individual incidences experienced in some organisations growing. The increase in number of incidences in Kenya could be attributed to technological transformation particularly following the growth of mobile phone platforms to transfer money among other services offered. This coupled with the uptake of card and online transactions as a means of settling payments has become an easy target for “tech savvy” fraudsters.
Fraud perpetrators in Kenya are getting bolder and targeting larger sums of money.

Cost of economic crimes

According to 55% of respondents who reported suffering economic crime in 2014, the impact of economic crimes in Kenya is still less than US$100k at organisational level. The percentage increase in the higher cost bracket (US$100k to US$5m) on the other hand signals some warning signs with indicated response levels of 25% in 2011 up to 34% in 2014. This could indicate that fraud perpetrators in Kenya are getting bolder and targeting larger sums of money which is generally in line with the recently reported incidences of economic crimes in the country.

Cybercrime, in particular, offers fraudsters an increased level of anonymity and convenience, and provides them access to larger pools of “virtual money” compared to traditional types of economic crime. In addition, economic pressures created by price inflation of food and other goods and services in the last two years and increases in interest rates may have contributed to the increase in the cost of economic crime.

These results could also be explained by the results obtained in relation to the profile of fraudsters. These seem to indicate that more members of middle and senior management are involved in economic crime. Economic crimes perpetrated at the level of middle and senior management are likely to involve larger sums of money than those at lower levels.

Survey respondents also assessed the impact of significant frauds in their organisations. Responses showed that in their assessment, employee morale was most affected (see table overleaf). According to respondents, the impact of economic crimes on business relations and reputation/brand was also significant.
The table above highlights the respondents’ measure of impact to their respective organisations. The impact of economic crime is likely to be felt on a much wider scale within the economy, affecting consumer and business confidence, causing financial loss and restricting business practices. In PwC’s 2013 *Africa Business Agenda*, 65% of CEOs in Africa and 84% of CEOs in Kenya expect to invest significantly in managing corporate reputation this year. It is worrisome that a relatively low percentage of Global Economic Crime respondents in Kenya (16%) perceive the potential impact of fraud on their organisations’ reputation and brand1.

For instance, survey results indicate that the prospect of setting up in a country perceived to be prone to corruption prompted 69% of respondents to undertake additional due diligence. This additional process implies that extra costs would be incurred by the organisation and this could be a possible deterrent to new firms planning to invest in such markets, or for existing firms exploring additional and new services.

While this survey focuses on economic crimes in individual organisations, there are instances where some organisations engage in joint and group economic crimes. In such cases the cost of the economic crimes may be higher and in most cases, the impact cascades to the wider public.

Shift from the “big three” to “big five”
Types of fraud suffered

Global and local surveys conducted in the past showed that three main types of economic crimes occurred most frequently - asset misappropriation, accounting fraud and bribery and corruption often referred to as the “Big three”. However, the 2014 survey results demonstrate that procurement fraud and cybercrime have gained prominence, resulting in a shift from the “Big three” to the “Big five” types of economic crimes. Below we include the Big five as well as the incidence rates reported for each type of economic crime according to our survey respondents.

<table>
<thead>
<tr>
<th>Type of Fraud</th>
<th>Incidence Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset misappropriation</td>
<td>77%</td>
</tr>
<tr>
<td>Accounting fraud</td>
<td>38%</td>
</tr>
<tr>
<td>Bribery and corruption</td>
<td>27%</td>
</tr>
<tr>
<td>Procurement fraud</td>
<td>31%</td>
</tr>
<tr>
<td>Cybercrime</td>
<td>22%</td>
</tr>
</tbody>
</table>

Although this shift has occurred, asset misappropriation is still the most widespread type of economic crime according to our respondents.

Asset misappropriation
Asset misappropriation remains the most frequently reported type of economic crime globally. In Kenya, among the survey respondents who reported economic crime, 77% (73% in 201) indicated asset misappropriation as the most prevalent form of fraud in their organisations. Prominence of asset misappropriation could be attributed to the fact that a wide range of irregularities can be easily classified under this type of economic crime and the opportunity to commit this type of irregularity is available to individuals at all levels of the organisation. Other types of economic crimes such as accounting fraud can be committed only by those individuals who are in a position to influence the financial statements.

Accounting fraud
Accounting fraud is the second most frequently reported type of fraud. This may involve accounting manipulations, fraudulent borrowings/raising of finance, fraudulent application for credit and unauthorised transactions/rogue trading. In 2014, the number of respondents reporting accounting fraud in Kenya remained steady at 38% similar to 2011. However 38% is still higher than the global average of 22%. Accounting fraud is most commonly perpetrated by more senior members of an organization, such as executives and senior staff. The reported high incidences of accounting fraud are characteristic of inadequacy of governance structures in organisations.
Bribery and Corruption

According to the Kenyan respondents to the 2014 survey, bribery and corruption accounted for 27% of economic crimes in their organisations, which is a marginal increase from 23% in 2011. Kenyan results are in line with the global average at 27% but significantly lower than the African average of 39%. It is important to note the context of these results – the survey measured the extent to which individuals experienced bribery/corruption in their own organisations, not in a macro sense.

It is concerning to note the slight increase of 4% from 2011 for bribery and corruption. Although not directly linked to the results of this survey, changes were recently made to the Kenyan constitution where more emphasis is placed on accountability of allocated resources as well as strengthening of the judiciary and other organs fighting corruption. This may be indicative of the fact that bribery and corruption are concerning economic crimes even in the wider public and regulatory platform. According to a separate study on bribery and corruption, PwC’s Africa Business Agenda indicates that a significant 75% of Kenya CEOs view bribery and corruption as a threat to growth.

Procurement fraud

For the first time, the 2014 survey included procurement, human resource and mortgage fraud as new economic crime classifications in the survey. Results for procurement fraud are worrying. Of the surveyed respondents in Kenya who had suffered economic crime, 31% reported having experienced procurement fraud. This is in line with the global average of 29% and lower than the African average of 43%.

Further analysis of procurement fraud occurrence indicates that 80% of the respondents cited vendor selection process as being more vulnerable to procurement fraud. This is above both the global average of 61% and the Africa average of 67%. After vendor selection, Kenya respondents’ cited vendor contracting (55%), bid process (45%), payment process (25%) and quality review (25%) as other processes that are under attack by fraudsters. This indicates that procurement fraud is perpetrated earlier in the procurement cycle making detection of such crimes difficult. It also shows that those who commit procurement fraud are strategically positioning themselves early in the procurement cycle.

A possible remedy is for organisations to have clearly set out vendor selection processes such as documenting clearly the rationale adopted in selection of a particular vendor including documentation of the same, more segregation of duties, utilization of specialised/customised procurement systems. Governance structures are also important – particularly those that ensure sufficient oversight of the procurement process or those that split the process so that a few individuals are not empowered to make decisions on the entire procurement process.

Cybercrime

Cybercrime is still a key concern to organisations in Kenya with 22% of the respondents reporting this crime. This is lower than the global average of 24%. Details of cybercrime are covered later in the report.
We can expect a higher cost of economic crime when the profile of the perpetrator is within middle/senior management.

Who is doing it? And how are they dealt with?

Internal fraudster
Similar to previous survey trends, most economic crimes are still committed by internal fraudsters. According to survey respondents who suffered economic crimes in Kenya, internal fraudsters were responsible for 61% of the cases, a decline from 2011 results of 68%. The Africa and global respondents average for internal fraudsters stood at 63% and 56% respectively.

<table>
<thead>
<tr>
<th>Level of internal fraudster</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Middle Management</td>
<td>54%</td>
</tr>
<tr>
<td>Junior Staff</td>
<td>28%</td>
</tr>
<tr>
<td>Senior Management</td>
<td>13%</td>
</tr>
<tr>
<td>Other</td>
<td>5%</td>
</tr>
</tbody>
</table>

Out of the internal perpetrators of fraud, members of the middle management accounted for more than half of all economic crimes at 54% according to respondents from Kenya. Junior staff accounted for 28% and senior management, 13%. These survey results are in line with the global trends but differ from the past where in 2011 Kenyan respondents reported internal fraudster at 42% for both middle level management and junior staff.

As discussed earlier, the above results might explain the increased cost of economic crime reported above. Middle management are likely to have more discretion over larger sums and are more likely to collude with external parties in committing economic crime. As a result, we can expect a higher cost of economic crime when the profile of the perpetrator is within middle/senior management.

External fraudster
Agents and intermediaries still lead the pack of external fraudsters according to 46% of 2014 respondents who experienced economic crimes in Kenya which significantly varies from the global average of 18%. This is followed by customers at 33% which matches the global average of...
32%. Agents and intermediaries being the primary external fraudsters would suggest that changes in business models where more processes are being outsourced mean organisations are increasingly becoming vulnerable to fraudulent activities. Close monitoring and enhanced controls are needed when dealing with subcontractors. The result raises questions on the extent to which organisations in Kenya have put in place robust governance structures and controls in dealing with agents and intermediaries.

In our experience, economic crime is often the product of collusion between internal and external perpetrators.

**Actions taken against perpetrators**

The preferred action taken when dealing with internal fraudsters is still dismissal at 85% according to the respondents in Kenya which mirrors global responses at 79% while Africa reported 76%. The rise in the tendency to dismissals as a response to incidences of internal fraud from 81% in 2011 to 85% in 2014 might suggest that organisations are taking firm stances against perpetrators of crime. Informing law enforcement agencies came second at 56%. There was a significant decline in the number of respondents taking civil action including recoveries from 54% in 2011 to 36% in 2014. This may be as a result of the dismal success rate in as far as civil proceedings are concerned.

The need to focus on suitable fraud response mechanisms and investigation approach that would aid in effective gathering of credible evidence that would lead to successful civil and criminal proceedings cannot be overemphasised. Alternatively the reduced tendency to seek civil action could also indicate unwillingness by organisations to start civil action that could lead to recovery due to the lengthy and costly legal processes in Kenya.

When dealing with external perpetrators of fraud, notifying relevant regulatory authorities is important in Kenya for 58% of respondents while informing law enforcement agencies is key for 54%. Only 50% of respondents ended the business relationship with the external party that perpetrated the fraud. This appears low but may suggest alternative avenues of recovery from external parties or a reliance on them. The percentage of African and Global respondents who took this action is also low at 31% and 37% respectively. Similar to internal fraudsters, only 38% of the Kenyan respondents would consider civil action against external perpetrators.

**Profile of a typical fraudster**

So who is your typical fraudster? Similar to past survey results a typical fraudster in Kenya is mainly an internal perpetrator (61%) from middle level management (54%), a male (85%) aged between 31 to 40 years (54%), who has been in his role for a period of between three to five years (44%) and possesses a first degree (69%).
The enemy hiding in plain sight

Practitioners commonly refer to a “Fraud Triangle” — the three elements that are often present when a perpetrator commits fraud: pressure, opportunity and rationalisation.

Three quarters (73%) of our respondents indicated that the opportunity or ability to commit the crime was the factor that most contributed to economic crime by an internal fraudster. Of the three factors, opportunity is the one most within an organisation's control.

This is a good thing. While life’s pressures and the ability to rationalise may swirl around employees, if an organisation can limit the opportunity, they may be able to stop the fraud before it starts.
16%

Of Kenyan respondents say that suspicious transaction reporting remains an effective way to detect fraud.

To Catch a Thief

So how do you stop an economic crime in progress — or better yet, before it happens?

The method of fraud detection usually falls into one of three categories: corporate controls; corporate culture; or happenstance. The figure below displays how major fraud at responding organisations was detected.

Suspicious transaction reporting still remains an effective way of detecting fraud according to 16% of Kenya respondents followed by routine internal audits at 14%, then fraud risk management at 13% and tip offs both external and internal at 14%.

In Kenya, a marginal increase of 3% was reported in the use of fraud risk management as a way of detecting economic crime, showing limited uptake of the practice.

More emphasis should be placed in strengthening internal audit functions and conducting regular fraud risk assessments as a way of early detection or prevention of economic crimes.

![Detection of Fraud Diagram](image-url)
It is perturbing to note that Kenyan respondents reported a decrease in the frequency of conducting fraud risk assessments.

**Fraud risk assessments and cybercrime**

**Fraud Risk Assessments**

Fraud risk assessments are used to ascertain whether an organisation has undertaken an exercise to consider:

- the fraud risks to which its operations are exposed,
- an assessment of the most threatening risks, that is, an evaluation of risks for significance and likelihood of occurrence,
- identification and evaluation of the controls that are in place to mitigate the key risks,
- assessment of the general anti-fraud programmes and controls in an organisation and
- actions to remedy any gaps in the controls.

Our survey results show that organisations have reduced the frequency with which they perform fraud risk assessments with a total of 25% not conducting any form of fraud risk assessment at all (19% in 2011). In Kenya 52% of respondents still conduct some form of fraud risk assessment at least once a year although this has also reduced from 78% in 2011.

This table is a comparison of the results from the 2014 and 2011 surveys.

<table>
<thead>
<tr>
<th>Frequency of fraud risk assessments</th>
<th>2014</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all</td>
<td>25%</td>
<td>19%</td>
</tr>
<tr>
<td>Once</td>
<td>23%</td>
<td>33%</td>
</tr>
<tr>
<td>Every six months</td>
<td>7%</td>
<td>11%</td>
</tr>
<tr>
<td>Quarterly</td>
<td>17%</td>
<td>28%</td>
</tr>
<tr>
<td>More often</td>
<td>5%</td>
<td>6%</td>
</tr>
</tbody>
</table>

The table shows us that respondents in 2014 indicated that the frequency of carrying out fraud risk assessments has reduced from 2011. In fact, 39% of respondents indicated that the reason they did not perform a fraud risk assessment is because they were not sure what it involved (down from 59% in 2011), while a further 16% did not see the value in performing one (29% in 2011).
As a trend from 2011, it appears that organisations have not realised the intrinsic value in fraud risk assessments. Some organisations are unaware of what exactly a fraud risk assessment involves, which suggests that more needs to be done to educate organisations on the value, effectiveness, quality and necessity of regularly performing fraud risk assessments.

It is perturbing to note that Kenya respondents reported a decrease in the frequency of conducting fraud risk assessments. This is contrary to the global trend where organisations and states (through legislation and specific requirements for government bodies) have put more emphasis on the need to undertake proactive fraud prevention measures such as a fraud risk assessment. The poor Kenyan record may be attributed to, among others, the following:

- the reactive nature of most organisations to fraud,
- insufficient knowledge and understanding of the concept of fraud prevention by most organisations,
- the reluctance by most organisations to commit resources (financial, personnel, infrastructure, etc.) towards combating fraud and
- a lack of regulatory and/or legislative obligation to implement proactive fraud prevention measures.

While a fraud risk assessment may be a fundamental proactive fraud prevention technique, there are other techniques that organisations may apply to address the risk of fraud and other related economic crimes. These include fraud risk management strategies, fraud prevention plans, fraud detection reviews, whistleblowing policies and hotlines. It is important to highlight the components of these proactive fraud prevention techniques which are prevention, deterrence, detection and response.
Cybercrime

Cybercrime, also known as a computer crime, is an economic crime committed using computers and the internet. Many smart phones and tablets have computer-like capabilities with the advancements in mobile device technology. So this definition of cybercrime can be extended to the and is very relevant in the Kenyan context where growth in the use of mobile phones has provided computing ability and internet access to a large proportion of the Kenyan population.

Cybercrime includes distributing viruses, illegally downloading files, phishing and pharming, and stealing personal information like bank account details. The definition of cybercrime is limited to crimes where a computer/mobile device and the internet play a central role in the crime and not an incidental one.

As we saw in PwC’s 2013 Africa Business Agenda, Africa is not immune to business results being impacted by a minefield of cyber risks including systems failures, security breaches and intellectual property abuse (privacy). The report highlights the need to increase use of audits and the establishment of necessary programmes to track and respond to these risks favourably3.

Twenty two (22%) of Kenyan respondents who reported having suffered economic crime had suffered a cybercrime incident. While this is a great concern, it must be noted that in many cases the victims of cybercrime may not even be aware of the incident. The actual incidence rate of cybercrime is likely to be much higher than what is reported. We asked survey respondents how their perception of the threat of cybercrime had changed over the last two years.

This chart shows the perception of the risk of cyber crime to our survey respondents.

In the survey, 50% of the respondents in Kenya stated that they perceive the risk of cybercrime has increased in the last 24 months (57% in 2011). In addition, 43% of the respondents in Kenya stated that their perception had remained the same.

A majority of the respondents indicated the threat of cybercrime was coming from both internal and external sources (49% in Kenya and 37% in Africa) whereas only 27% of respondents in Kenya and 41% in Africa indicated the threat as only coming from external sources. Despite the source of the threat, it is clear that respondents were concerned about the impact of cyber crime on various aspects of their organisations.

**This table summarises these concerns.**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft or loss of personal identity information</td>
<td>10%</td>
<td>8%</td>
<td>8%</td>
<td>15%</td>
</tr>
<tr>
<td>Actual financial loss</td>
<td>10%</td>
<td>8%</td>
<td>8%</td>
<td>15%</td>
</tr>
<tr>
<td>Reputational damage</td>
<td>10%</td>
<td>8%</td>
<td>8%</td>
<td>15%</td>
</tr>
<tr>
<td>Service disruption</td>
<td>10%</td>
<td>8%</td>
<td>8%</td>
<td>15%</td>
</tr>
<tr>
<td>IP theft, including theft of data</td>
<td>10%</td>
<td>8%</td>
<td>8%</td>
<td>15%</td>
</tr>
<tr>
<td>Legal, Investigation and/or Enforcement Costs</td>
<td>10%</td>
<td>8%</td>
<td>8%</td>
<td>15%</td>
</tr>
<tr>
<td>Regulatory risks</td>
<td>10%</td>
<td>8%</td>
<td>8%</td>
<td>15%</td>
</tr>
</tbody>
</table>

The cybercrime threat is constantly evolving, with cyber criminals changing their methods and using newer technologies over time. In this context, cyber security is a constantly moving target for organisations. Even then, organisations continue to make their critical data available to management, employees, vendors, and clients on a multitude of platforms because the economic and competitive benefits appear so compelling. These include high risk platforms such as mobile devices and the cloud.

The key question is what possible measures can be taken to address these concerns. PwC’s cyber security experts recommend keeping the following key messages in mind when designing a Cybercrime Response Strategy (CcRS).

- **Assume a state of compromise** – A CcRS should be designed from the point of view that internal systems have already been breached. Adopt the philosophy of an assumed state of compromise, focusing on continuous detection and crisis response in addition to the more traditional IT security focus of protection and mitigation.
• Identify the “crown jewels” or critical assets. Allocate and prioritise resources to protect your most valuable information. Ensure their location is known and access to them is controlled and monitored effectively.

• Conduct regular security assessments to detect cyber attacks. These assessments should be risk based and focused and should seek to identify areas that can be exploited by internal and external parties for personal gains.

• Have an incident management plan. Planning and preparedness should be improved through table-top simulations of recent industry events and likely attack scenarios. These should be frequently conducted. Potential response to various attack scenarios and crisis should be pre-scripted in a play book format.

• PwC’s 2011 Delusions of safety report indicates the need for new structures, roles and governance and a new mindset focused on protecting the organisation and its wider ecosystem. The report reinforces that this needs to be driven from the top with the need for greater board level awareness of the challenge. Cybercrime should not be viewed as an IT challenge but as a global business challenge. It should be embedded into the executive decision making process. A cybercrime response plan should integrate both IT and business responses and elicit the participation of all parts of the business from the executive team to the legal, communications and human resources teams.

• Cyber security is no longer about keeping the attacker out, it also requires an understanding of the threats and being able to respond when it happens. Organisations need to have a system that is able to deter, defect and respond to fraud.

Perception of corruption, money laundering and competition/anti-trust law

The 2014 survey introduced a new area relating to respondents’ relative perceptions of three major economic issues. These are corruption, money laundering and competition law. These economic issues affect organisations across the globe and have a strong impact on businesses and individuals.

The table below shows the relative perceptions of Kenya respondents as to which of these three economic issues posed the highest risk to doing business globally. Fifty two percent (52%) of Kenya respondents believed corruption posed the highest risk to doing business globally while 62% of Kenyan respondents believed that competition law posed the lowest risk to global business. This may indicate the less developed competition law frameworks in Kenya, as compared to Western European or American economies where these have a greater impact on the economy. Global results for corruption were not significantly different from those of Kenyan respondents, but more global respondents perceived a greater risk from competition law, though the ranking remained the same.
Corruption was perceived by Kenyan respondents as having the most severe impact to their organisations in terms of financial loss and loss of reputation (38% and 34% respectively). Interestingly, 22% of Kenyan respondents perceive the impact of competition law on their businesses as a distraction. This data is captured in the table below.

Africa had the highest percentage of respondents (61.2%) ranking corruption and bribery as the highest risk to the organization. Western Europe had the highest percentage of respondents (25.3%) rank competition/anti-trust law as the highest risk to the organization, while Eastern Europe also ranks competition/anti-trust law fairly highly with 24.5% of respondents in the region ranking it highest. Across key industries, bribery and corruption remains the highest risk in doing business globally, with the exception of financial services where 57.6% of respondents within the industry ranked money laundering as the highest risk to the organisation.

The survey also explored the incidence of bribery among respondents. The table below shows the results of the survey in this respect.

36% of Kenyan respondents had been asked to pay a bribe in order to get business.
Thirty six percent (36%) of the respondents in Kenya indicated they had been asked to pay a pay a bribe in order to get business. An additional 45% indicated they had lost business to a competitor who they believed paid a bribe. These are twice as high as our global responses where the figures were 18% and 22% respectively. Our Global respondents (53%) indicated that they had not been asked to pay a bribe, this figure is only 32% in Kenya.

Fifty three percent (53%) of Kenyan respondents stated they had actively pursued opportunities in markets with a high level of corruption risk. Out of these 38% indicated that they had to change their business strategy in order to pursue the opportunity. For 68% of these respondents, this mainly involved carrying out additional due diligence whereas 42% indicated they altered their terms of business. Thirty eight percent (38%) of respondents who pursued opportunities in markets which they perceived had a high level of corruption risk indicated they walked away from these opportunities.

These results give an indication of the wider economic impact of economic crime, particularly bribery. The survey results show that, aside from the financial loss bribery causes it may also restrict consumer choice and stifle growth by preventing expansion into new markets and new products.

**Bribery and corruption – the Global perspective**

An extract from our Global GECS 2014 report

“It is easy for those who have lived in relatively corruption free societies to underestimate the significance and power of cultural norms related to the “demand side” of corruption. It is likely that when your employees are challenged with sales and other business goals with “high corruption demand,” they may not perceive the risk of participating in a corrupt scheme with the expected, and required, degree of caution.

Accordingly, they are likely to find a wide variety of means and rationalisations for following the local customs, as opposed to abiding by corporate policies.

This continuing contest between corporate expectations and local cultural norms is not as easy to win as many expect. It is this dynamic that threatens your sales and marketing processes by pressuring personnel into improper contracts, adds unnecessary layers in the distribution channel, allows “quid pro quo” transactions like hiring relatives of customer executives, creating marketing or advisory roles for customer employees, or increasing the discount to a distributor or travel agent to create a “slush” fund.

Overcoming the power of local cultural expectations requires a strong and consistent message to all employees to achieve the right balance between your employees’ life experience and work experience.”
Conclusions

A bold approach to tackling economic crime in today’s world is not an option – it’s an imperative.

Our 2014 survey results have brought interesting trends in economic crime to light. These trends can be used to assist you to identify vulnerabilities and accordingly, strengthen processes and develop robust systems to deter, detect and deal with economic crime in your organisation.

In formulating such systems, the engagement and tone of senior management and executives is of paramount importance in their success. These systems need to be constantly evaluated and reviewed in the face of the changing techniques employed by fraudsters and technological advancements.

Fraud prevention measures will also be key in acting as a deterrent and in the detection of economic crime. The Kenyan responses in our survey indicate that a lot more can and needs to be done with regard to the preventative aspects of combatting economic crime in Kenya.

The shift from the “Big three” to the “Big five” indicates that cyber security and increased monitoring of business processes, particularly finance and procurement should be at the top of the agenda for management. This combined with strengthened governance mechanisms particularly in the Kenyan context, could be a first step for organisations in their fight against economic crime.

Taking a proactive approach to economic crime is critical. Aside from the measurable financial losses, we must take into account the wider impact. This includes the opportunity costs of its effects on competition and the deterrent it creates with regards to entry into new markets and provision of new services.

We cannot discount the impact to the wider economy of a more secure business community, and the confidence this would create. A bold approach to tackling economic crime in today’s world is not an option – it’s an imperative.
Methodology

We carried out our seventh Global Economic Crime Survey between August 2013 and February 2014.

The survey had four sections:
• general profiling questions,
• comparative questions looking at what economic crime organisations had experienced,
• cybercrime fraud threats and
• corruption/bribery, money laundering and competition law/anti-trust law.

About the survey

The 2014 Global Economic Crime Survey was completed by 5,128 respondents (compared to 3,877 respondents in 2011) from 95 countries (compared to 78 countries in 2011). Of the total number of respondents, 50% were senior executives of their respective organisations, 35% represented listed companies and 54% represented organisations with more than 1,000 employees.

We used the following research techniques

1. **Survey of executives in the organisation.** The findings in this survey come from executives’ reports of their experiences of economic crimes in their organisations. We obtained information from them on the different types of economic crime, their impact on the organisation (both the financial loss and any collateral damage), the perpetrator of these crimes, what action the organisation took and how they responded to the crime.

2. **Questions relating to cybercrime, corruption/bribery, money laundering and competition law/anti-trust law.** This survey takes a detailed look at these threats which are often systemic in nature and thus are more prone to have a long term, damaging impact on the organisation.

3. **Analysis of trends over time.** Since we started doing these surveys in 2001, we have asked a number of core questions, and extra ones that are relevant from time to time, dealing with issues likely to have an impact on organisations around the world. With this historical data on hand, we can see current themes, chart developments, and find trends.

Other Resources

• PwC - 2013 Africa Business Agenda, 3rd Edition (www.pwc.com/theagenda)
• PwC - 2011 Delusions of Safety- The Cyber Savvy CEO (http://www.pwc.com/gx/en/psrc/global/cyber-savvy-ceo-report.jhtml)
Terminology

Accounting fraud
Financial statements and/or other documents are altered or presented in such a way that they do not reflect the true value or financial activities of the organisation. This can involve accounting manipulations, fraudulent borrowings/raising of finance, fraudulent application for credit and unauthorised transactions/rogue trading.

Asset misappropriation, including embezzlement/deception by employees
The theft of assets (including monetary assets/cash or supplies and equipment) by directors, others in fiduciary positions or an employee for their own benefit.

Bribery and Corruption
The unlawful use of an official position to gain an advantage in contravention of duty. This can involve the promise of an economic benefit or other favour, the use of intimidation or blackmail. It can also refer to the acceptance of such inducements. Specific examples include kickbacks, extortion, gifts (with strings attached), facilitation payments, etc.

Competition Law/Anti-Trust Law
To promote or maintain market competition by regulating anti-competitive and unfair business practices conducted by organisations. Examples may include price fixing, excessive, predatory or discriminatory pricing, unfair trading terms, and tying (i.e., stipulating that a buyer wishing to purchase one product must also purchase all or some of his requirements for a second product).

Cybercrime
Also known as computer crime, cybercrime is an economic offence committed using the computer and internet. This can be widened to include mobile devices with computing capability. 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.

Economic crime
The intentional use of deceit to deprive another of money, property or a legal right.

Espionage
Espionage is the act or practice of spying or of using spies to obtain secret information.

Financial loss
When estimating financial losses due to fraud, the participants should include both direct and indirect loss. The direct losses are the actual amount of fraud and the indirect losses would typically include the costs involved with investigation and remediation of the problem, penalties levied by the regulatory authorities, and litigation costs. This should exclude any amount estimated due to “loss of business opportunity”.

Financial terms
When estimating financial losses due to fraud, the participants should include both direct and indirect loss. The direct losses are the actual amount of fraud and the indirect losses would typically include the costs involved with investigation and remediation of the problem, penalties levied by the regulatory authorities, and litigation costs. This should exclude any amount estimated due to “loss of business opportunity”.

Fraud risk assessment
Fraud risk assessments are used to ascertain whether an organisation has undertaken an exercise to specifically consider:

- the fraud risks to which operations are exposed,
- an assessment of the most threatening risks (i.e., Evaluate risks for significance and likelihood of occurrence),
- identification and evaluation of the controls (if any) that are in place to mitigate the key risks,
- assessment of the general anti fraud programmes and controls in an organisation and
- actions to remedy any gaps in the controls.

Human Resources fraud (recruitment and/or payroll fraud)
Fraud committed by members of the Human Resources department, including payroll fraud, ghost employees, pay-to-work, recruitment (i.e., hiring friends and/or relatives, hiring unqualified individuals, falsification of documents, etc.).
**Incentive/Pressure to Perform**
The individual has some financial problem that he/she is unable to solve through legitimate means so he/she begins to consider committing an illegal act as a way to solve the problem. The financial problem can be professional (e.g., job is in jeopardy) or personal (e.g., personal debt).

**Insider trading**
Insider trading refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non public information about the security. Insider trading violations may also include ‘tipping’ such information, securities trading by the person ‘tipped’, and securities trading by those who misappropriate such information.

**IP infringement (including trademarks, patents, counterfeit products and services)**
This includes the illegal copying and/or distribution of fake goods in breach of patent or copyright, and the creation of false currency notes and coins with the intention of passing off as genuine.

**Markets with a high level of corruption risk**
While corruption risk levels can be subjective, for the purposes of this survey we suggest a territory with a Transparency International Corruption Perception Index (“CPI”) score of 50 or less be considered a market with a high level of corruption risk. This link [www.transparency.org/country](http://www.transparency.org/country) will direct you to the Transparency International list of territories and CPI scores. The 2013 Transparency International CPI score for Kenya is 27.

**Money laundering**
Actions intended to legitimise the proceeds of crime by disguising their true origin.

**Mortgage Fraud**
Mortgage fraud schemes employ some type of material misstatement, misrepresentation, or omission relating to a real estate transaction which is relied on by one or more parties to the transaction.

**Opportunity or ability**
The individual finds some way that he/she can use (abuse) his/her position of trust to solve the financial problem with a low perceived risk of getting caught.

**Procurement Fraud**
Illegal conduct by which the offender gains an advantage, avoids an obligation or causes damage to his organisation. The offender might be an employee, owner, statutory board member, an official, a public figure or a vendor who was involved in the purchase of services, goods or assets for the affected organisation.

**Rationalization**
The individual finds a way to justify the crime to himself/herself in a way that makes it an acceptable or justifiable act.

**Tax Fraud**
An illegal practice where an organisation or corporation intentionally avoids paying its true tax liability.
Contacts

Alphan Njeru  
Advisory Leader, Kenya  
+254 (020) 285 5111  
Alphan.njeru@ke.pwc.com

Muniu Thoithi  
Forensics Leader, Kenya  
+254 (020) 285 5684  
muniu.thoithi@ke.pwc.com

George Weru  
Senior Manager, Kenya  
+254 (020) 285 5360  
george.weru@ke.pwc.com

John Kamau  
Manager, Kenya  
+254 (020) 285 5065  
john.kamau@ke.pwc.com

Malvi Shah  
Manager, Kenya  
+254 (020) 285 5057  
malvi.shah@ke.pwc.com

Tshepo Nyatlo  
Manager, Kenya  
+254 (020) 285 5505  
tshepo.nyatlo@ke.pwc.com