# Fraud: The overlooked competitor

## 2018 Global Economic Crime and Fraud Survey

UGANDA REPORT

www.pwc.com/ug

# Foreword

***We are pleased to present the first ever Uganda GECS report***

**Francis Kamulegeya**
Senior Country Partner,
PwC Uganda

**Muniu Thoithi**
Forensics Leader,
East Africa Region

We are pleased to present the 2018 Global Economic Crime and Fraud Survey ("GECS 2018") report for Uganda. The Global Economic Crime and Fraud Survey ("GECS") is a biennial PricewaterhouseCoopers survey that receives and analyses feedback from stakeholders in various economic sectors of focus in relation to the nature, prevalence and effects of economic crimes experienced over the preceding 24 months of operations.

For the first time since the launch of the PwC GECS initiative 17 years ago, we are able to generate a country-specific report for Uganda, thanks to the increased level of participation in the Survey by Ugandan organisations.

In this current survey, we received responses from over 7,000 respondents across 123 countries in 18 languages. This makes GECS 2018 one of the largest and most comprehensive surveys on economic crime in the world.

The last 24 months have seen significant socio-economic and geopolitical developments on both the global and the local scenes that have shaped the backdrop against which the results of our most recent survey can be viewed. The period from October 2015 to October 2017 was marked by landmark votes in key Western economies. The United Kingdom voted in favour of "Brexit" in June 2016.

In November of that year the United States elected Donald Trump as President, who ran on an "America First" policy platform. Subsequently, perhaps more predictable elections took place in both France and Germany. Despite significant political change, the global economy grew by 2.6% in 2016  and is estimated to have grown at 3% in 2017 .

On the African stage, during the same period, Presidential elections took place in a number of Africa's "market hub" countries, such as Uganda, Kenya, Tanzania, Rwanda, Zambia and Ghana. In some cases the elections resulted in some uncertainty, but matters are gradually returning to normal. In addition, commodity prices fell for most of 2016 on the back of reduced Chinese demand, before showing some recovery in 2017.

The effect of this drop and subsequent rise was to dramatically lower and then somewhat increase the value of African commodity exports, so that sub-Saharan Africa's GDP growth dropped to 1.3% in 2016  before rising to 2.4% in 2017 .

Domestically, the annual GDP growth rate for the year 2016/17 was 4%, a 0.7% reduction from the 4.7% registered in 2016/17 according to Uganda Bureau of Statistics. In the medium term, the annual GDP growth rate in the five years leading to 2015/16 was 4.5% according to the World Bank. For the last two years, adverse weather conditions have affected agricultural productivity and impeded economic growth. This is due to the fact that as highlighted in the 2014 Uganda Population and Housing Census, 69% of Ugandan households depend on subsistence farming for a living.

In this report, we highlight the forms of economic crime most prevalent in Uganda, comparing them with the global survey results as well as the results for Africa and the East Africa region consisting of Uganda, Kenya, Tanzania, Rwanda and Zambia. The comparisons provide insights on the opportunities that exist for cross adoptions and cross learnings amongst different countries and regions.

In today's interconnected world, the comparison also provides a birds-eye-view of the economic crime environment in the region for organisations with cross-border operations, which is useful in forming fraud risk management strategies. Overall, Uganda respondents reported a 66% incidence rate in occurrence of economic crimes. Whereas this rate

***3 in 5 of Uganda respondents reported having experienced at least one form of economic crime in the past two years. I high incidence rate could be an indication of either a high prevalence or a high awareness of fraud***

is lower than the rates reported by organisations in countries such as South Africa and Kenya, it is nonetheless high when compared to the average prevalence rates in Africa (62%) and globally (49%). The high rates of economic crime incidence calls for proactive and stringent measures to counteract the fraud.

Among the forms of economic crime that were found to have a high prevalence rate within Ugandan organisations include Fraud Committed by the Consumer, Business Misconduct, Asset Misappropriation, Cybercrime and Bribery and Corruption. The first two forms of fraud primarily affect the private sector and it is imperative that the sector institutes measures aimed at curbing their prevalence. The prevalence of these particular crimes is not as high as in some of the other East African countries; it may be worthwhile therefore, for Ugandan organisations to assess whether there are any useful insights that can be borrowed from its neighbours.

Bribery and Corruption on the other hand has been perceived for a long time, and perhaps wrongly so, as a public sector problem. During his swearing-in speech in 2016, H.E. Yoweri Kaguta Museveni declared that there are two weaknesses that the country needs to expunge for the economy to perform well and one of them was corruption by public officials. According to the President, corruption and delayed decision making "irritate the public and frustrate investors". Shortly thereafter, the Government of Uganda removed more than 5,000 civil servants suspected to be ghost workers from the state payroll . Such bold steps are encouraging and should be sustained to rid Uganda of the vices of economic crimes.

Also encouraging as per our survey is the fact that a high proportion of Ugandan organisations seem to be investing in anti-fraud measures. For instance, 78% of respondents indicated that they have a fully operational cybersecurity programme. An impressive 85% of our respondents also reported having insight into fraud and/or economic crime incidence in their organisation.

Our survey reinforces the importance of all stakeholders converging in the fight against fraud. While the government must for instance ensure that there is a comprehensive and all-inclusive legal and enforcement framework in place, the private sector, civil society, religious leadership and indeed the entire citizenry must converge around the goal of eradication of economic crimes.

IWorld Trade and GDP Growth in 2016 and early 2017, World Trade Organisation

[2]Global Economic Prospects Broad-Based Upturn, but for How Long?, World Bank

[3]April 2017; "Africa's Pulse" (published by the World Bank)

[4]Kambou, G. (January 2018) The outlook for Sub-Saharan Africa in five charts: Striving for recovery. World Bank Blog

[5]http://www.theeastafrican.co.ke/news/Uganda-stops-paying-more-than-5500-ghost-civil-servants/2558-3340742-drd6mqz/index.html

# Contents

# Introduction

We are pleased to present our ninth biennial Global Economic Crime Survey ("GECS") Report and the first Uganda country report. The report aims to give you insights into the prevalence of economic crimes in the last 24 months, corporate attitudes towards them as well as the trends observed and motives behind economic crimes.

Carried out every 2 years globally since 2001, GECS collects and analyses feedback on economic crime from a multi-sectoral pool of organisation leaders. Country specific reports are generated for countries that achieve the minimum number of respondents required to allow for a statistically sound analysis of the results. In Africa, reports have previously only been available for South Africa, Kenya, Nigeria and Zambia and it is therefore with great pleasure that we add Uganda to this list.

**7,000**

Respondents from 123 countries in 18 languages

Globally, GECS 2018 analyses feedback from over 7,000 stakeholders in the economic sectors of focus across 123 countries and in 18 languages. This makes it one of the largest and most comprehensive surveys on economic crimes in the world. Drawing from this extensive pool, the GECS 2018 report aims to give you insights on the prevalence of economic crimes in the last 24 months.

In Uganda, the report draws insights from the experiences, perceptions and knowledge of economic crime from 64 respondents. The 64 respondents are Board Members and Senior Managers who are part of Executive Management, Finance, Audit, Risk Management and other core functions in large, medium and small organisations. Of the 64 respondents, 48% represent listed companies, 41% private organisations and 11% public or non-governmental institutions.

**64**

Respondents in Uganda and 379 in East Africa

In the age of globalization, the prevalence, control and effects of economic crimes in Uganda is to a significant extent affected by the geopolitical and socioeconomic conditions of the regional blocks it inhabits. This report therefore compares the survey results in Uganda to those observed in the East African Region (consisting of Uganda, Kenya, Tanzania, Rwanda and Zambia), Africa and globally and goes ahead to contextualize those results in light of the country's social, political and economic developments.

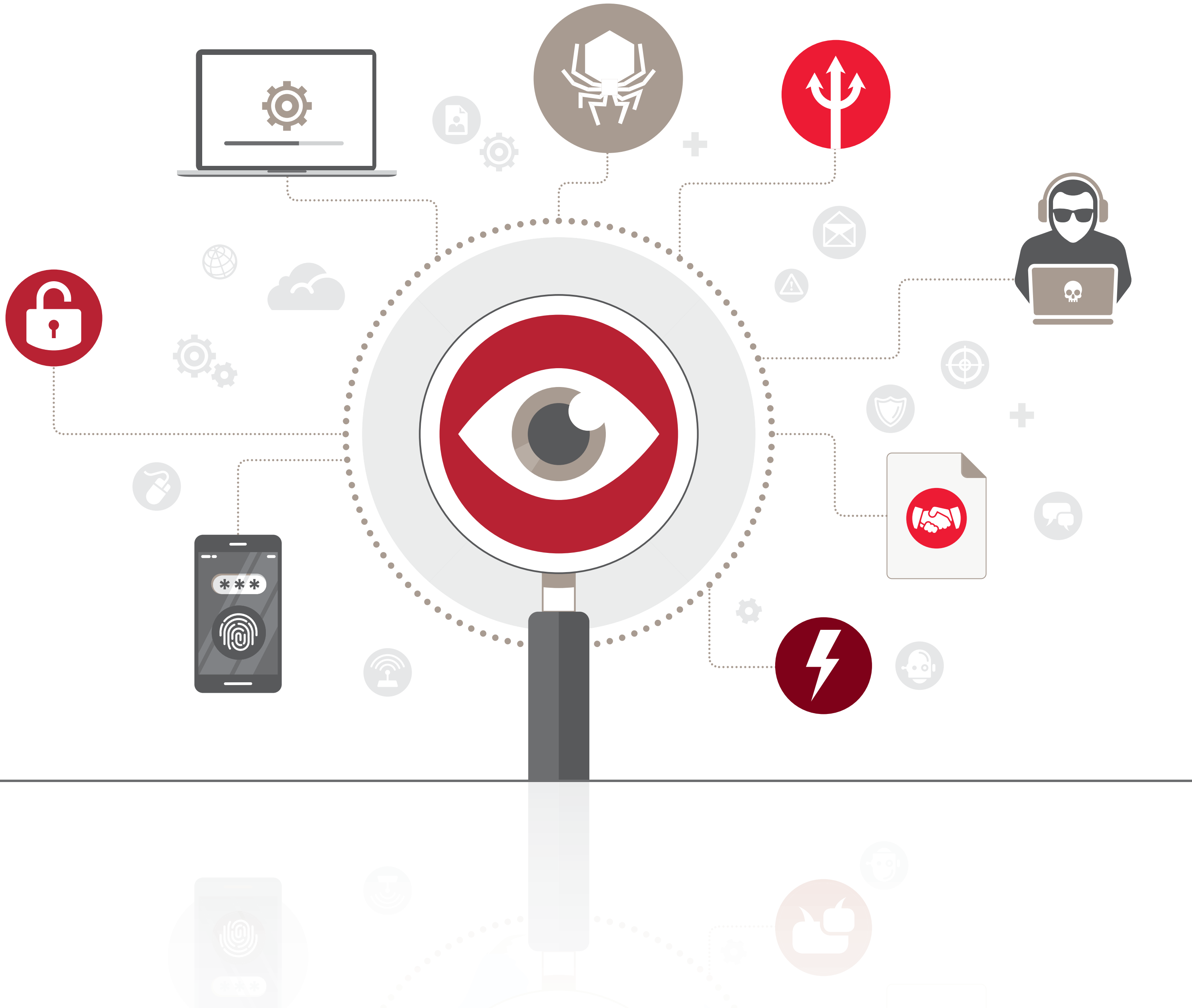
Ugandan organisations reported a 66% incidence rate of having experienced at least one form of economic crime over the last 24 months, which is 35% higher than the global average. Fraud Committed by the Consumer was the most prevalent economic crime in Uganda. This economic crime classification relates to fraud where a consumer in the course of undertaking a legitimate transaction with an organisation, exploits the governance and control weaknesses of the organisation to commit fraud. The results of the survey showed that this crime had a 45% incidence rate in Uganda. It was followed by Business Misconduct and Asset Misappropriation. Fraud Committed by the Consumer was especially prevalent in the Financial Services industry where it had an incidence rate of 57%.

In this report, we take a closer look at Fraud Committed by the Consumer as it counts as the most prevalent form of economic crime in Uganda. We also pay special attention to Cybercrime given that it ranks highest as the form of economic crime that is expected by the majority of respondents to be most disruptive over the next 24 months.

For organisations to effectively detect and prevent fraud, it is imperative to know who is committing the fraud. We therefore also present the survey findings in respect to the profile of the fraudsters. We note the prominence of the customer as the biggest external threat. Internally, middle level management was found to be responsible for almost half (45%) of the reported internal fraud.

We also discuss how organisations can manage and prevent economic crimes. Corporate controls and an open corporate culture were considered crucial for a majority of Uganda respondents as far as detection of economic crimes is concerned. As far as prevention is concerned, we consider emerging technologies such as artificial intelligence and machine learning as early warning systems and first lines of defence against economic crimes. Further, we investigate the drivers of internal fraud through the lens of The Fraud Triangle and extract useful insights including the need to pay close attention to corporate pressures, control and enforcement gaps and the organisational environment and culture.

# Painting the picture of Economic Crime



**66%**

of Uganda respondents experienced economic crime in the last 24 months, compared to 49% globally and 62% in East Africa

## Global, Regional and Local perspectives

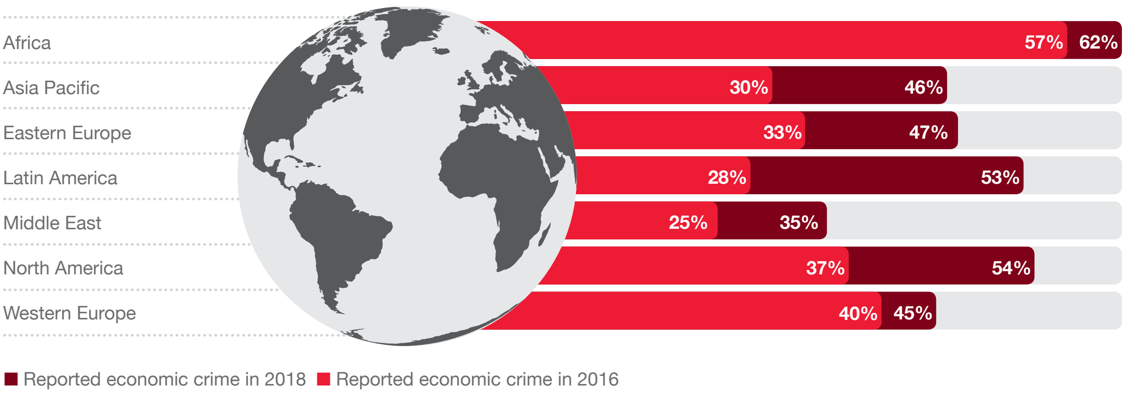
Globally, the 2018 Survey saw an increase in the proportion of respondents who reported having experienced an economic crime in the last 24 months of operations.

Half (49%) of our global respondents reported experiencing an economic crime in their area of work compared to 36% who reported the same in 2016.

the vices. Indeed, in terms of percentage increase in incidence of crime Africa had the lowest increase of 9% with Latin America recording the highest increase of 89% increase from 2016.

Of the 10 countries that reported the highest incidence rate of economic crimes globally, we observe that half are African Countries, once again bringing into focus Africa as a region that is most severely affected by economic crimes. Of the remaining five, three were European and a country each from Asia and Central America.

**The reported rate of economic crime has increased across all territories**

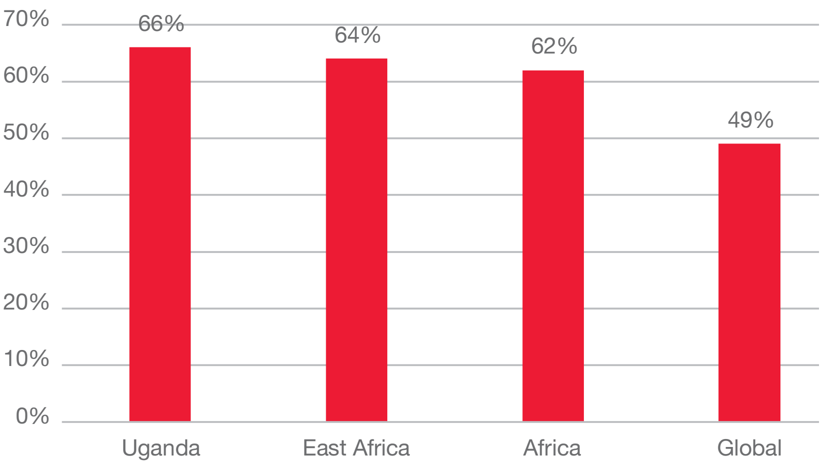



In Uganda, 66% of our respondents indicated that they had experienced at least one form of economic crime in the last two years.

Whereas Africa continues to take the lead in the pervasiveness of economic crimes in the last 24 months at 62% prevalence up from 57% in 2016, other regions were also not immune to the brunt of

It is not however necessarily all doom and gloom. The significant jump in reported fraud and the high prevalence in our region is not the whole story. In fact, it may be the opposite of the story. That is because forensics practitioners know that the real percentage of economic crime victimisation is significantly higher than the reported incidents — not 49% globally or 66% in Uganda.

**Incidence rates in 2018**




***All regions globally experienced an increase in incidences of economic crime as per the survey***

More likely, the reality is that this statistic measures not actual fraud, but awareness of fraud. Either way, however, the high prevalence rate in some countries and regions is a good measure of just how big a problem economic crime is seen to be in these countries.

## Forms of Economic Crime

As already noted, Fraud Committed by the Consumer ranks highest as the most prevalent economic crime experienced by survey respondents in Uganda. This seems to be in line with the finding that customers are the biggest contributors to fraud by external parties. We therefore discuss both Fraud Committed by the Consumer and the role of the customer in the section of this report entitled Customers – both friend and foe (on page 15).

Given that Cybercrime scored the highest among Uganda's respondents as the form of economic crime likely to be most disruptive to their organisations in the next 24 months, both monetarily and otherwise, we also discuss it in detail in the section Cybercrime – the crime of the future (page 18).

In this section, we briefly discuss some of the other forms of economic crime that were reported to be widely experienced by Ugandan organisations.

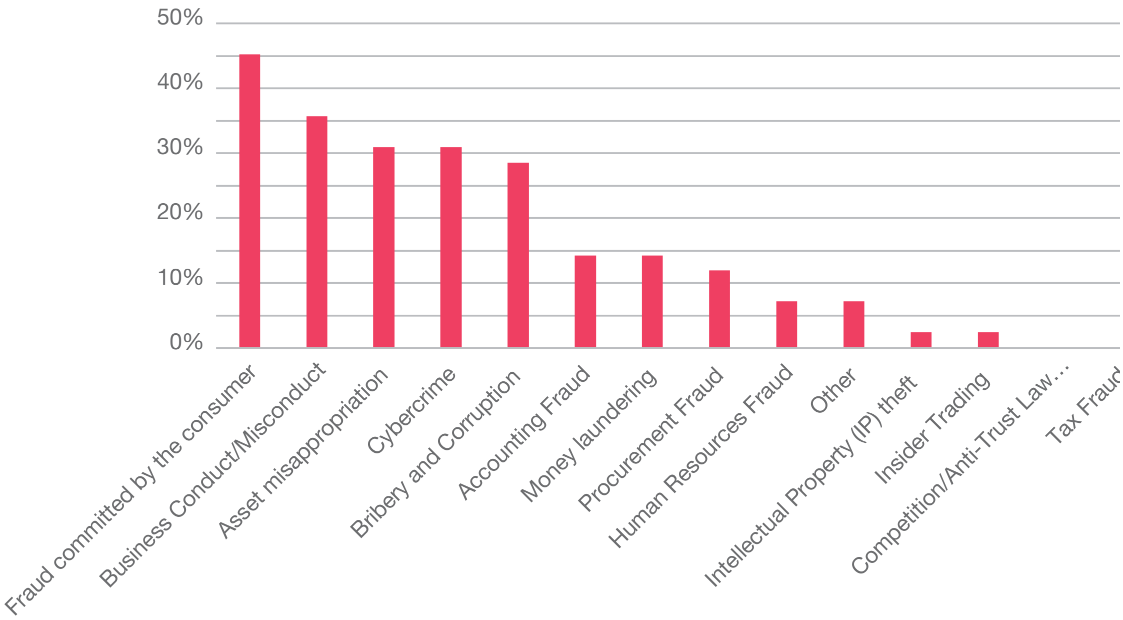
## Business Conduct/Misconduct – an unwanted Ugandan first place

Business Conduct/Misconduct refers to frauds or deception by companies upon the market or general public. It involves deceptive practices associated with the manufacturing, sales, marketing or delivery of a company's products or services to its clients, consumers or the general public.

It is the second most prevalent form of economic crime in Uganda with an incidence rate of 36%. This is compared to the 29% incidence rate in East Africa, 31% in Africa and 28% globally. The proportion of respondents that experienced incidents of Business Misconduct is thus observed to be larger in Uganda than that in the other comparators. This is a striking indication that something wrong is afoot and speaks to a likely gap in business ethics.

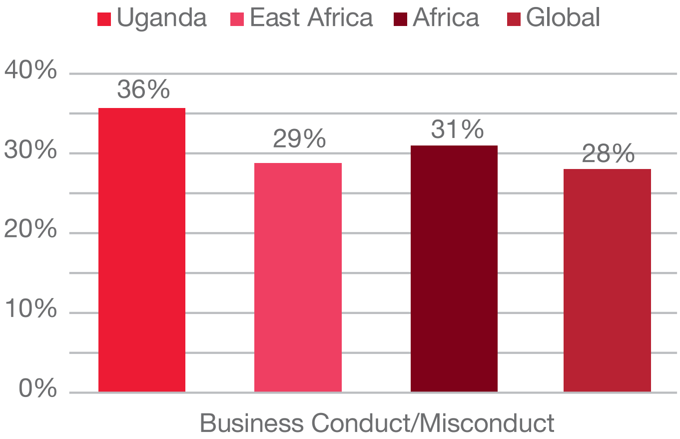
With a 17% incidence rate, Business Misconduct ranked as the third most disruptive form of economic crime experienced by the Uganda respondents over the last 24 months. Interestingly, the majority of respondents saw this form of crime as being less disruptive going forward with only 3% of respondents envisaging it to be the most disruptive form of economic crime in the next 24 months. Despite being highly prevalent and

**Incidences of Economic Crime in Uganda**




***Unlike her East Africa neighbours and the global trend, Asset Misappropriation was not the most prevalent form of economic crime in Uganda***

**Business Conduct/Misconduct in 2018**




disruptive, therefore, only a moderate proportion of respondents envisage Business Misconduct to be a persistent problem in the future. This leads us to ask a rather searching question: what is this confidence based on?

Going by the indications from the survey, it is likely that business leaders foresee a significant change in business attitudes probably brought about by increased scrutiny into corporate processes and products and the eventual business losses brought about by negative press in the marketplace. This, by all accounts, gives reason for hope and optimism over the next 24 months.

## Asset Misappropriation – the forgotten giant

Asset Misappropriation is a form of economic crime that involves the theft or embezzlement of company assets by directors, employees or other fiduciaries. The distinguishing feature of Asset Misappropriation from other forms of theft is that Asset Misappropriation does not involve the use of force. Rather, the perpetrator of the fraud relies on trickery and deceit to exploit the organisation's controls and transfer its assets to themselves or to the ownership of a third party, without the organisation's knowledge or consent.

This crime covers a wide range of nefarious acts ranging from the embezzlement of physical assets such as cash to embezzlement of non-cash proprietary information and intellectual property such as patents and copyrights.

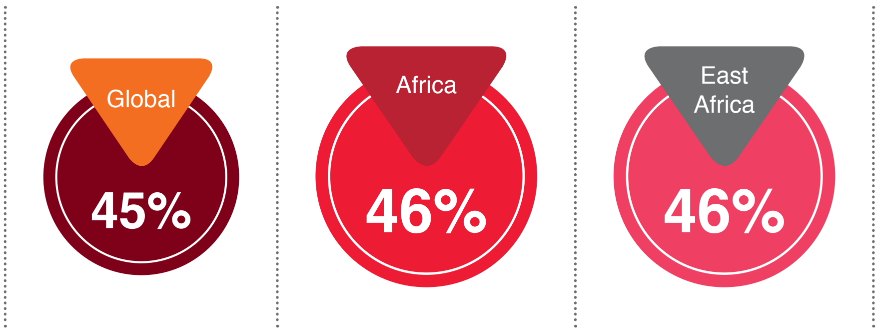
Asset misappropriation is the third most prevalent form of economic crime in Uganda, tying with Cybercrime with an incidence rate of 31%. This is against the twin 46% incidence rate in both East Africa and Africa and 45% globally.

It is instructive to note that Asset Misappropriation ranks as the most prevalent form of crime globally and in Africa, this is a position that it has held for the last few surveys.

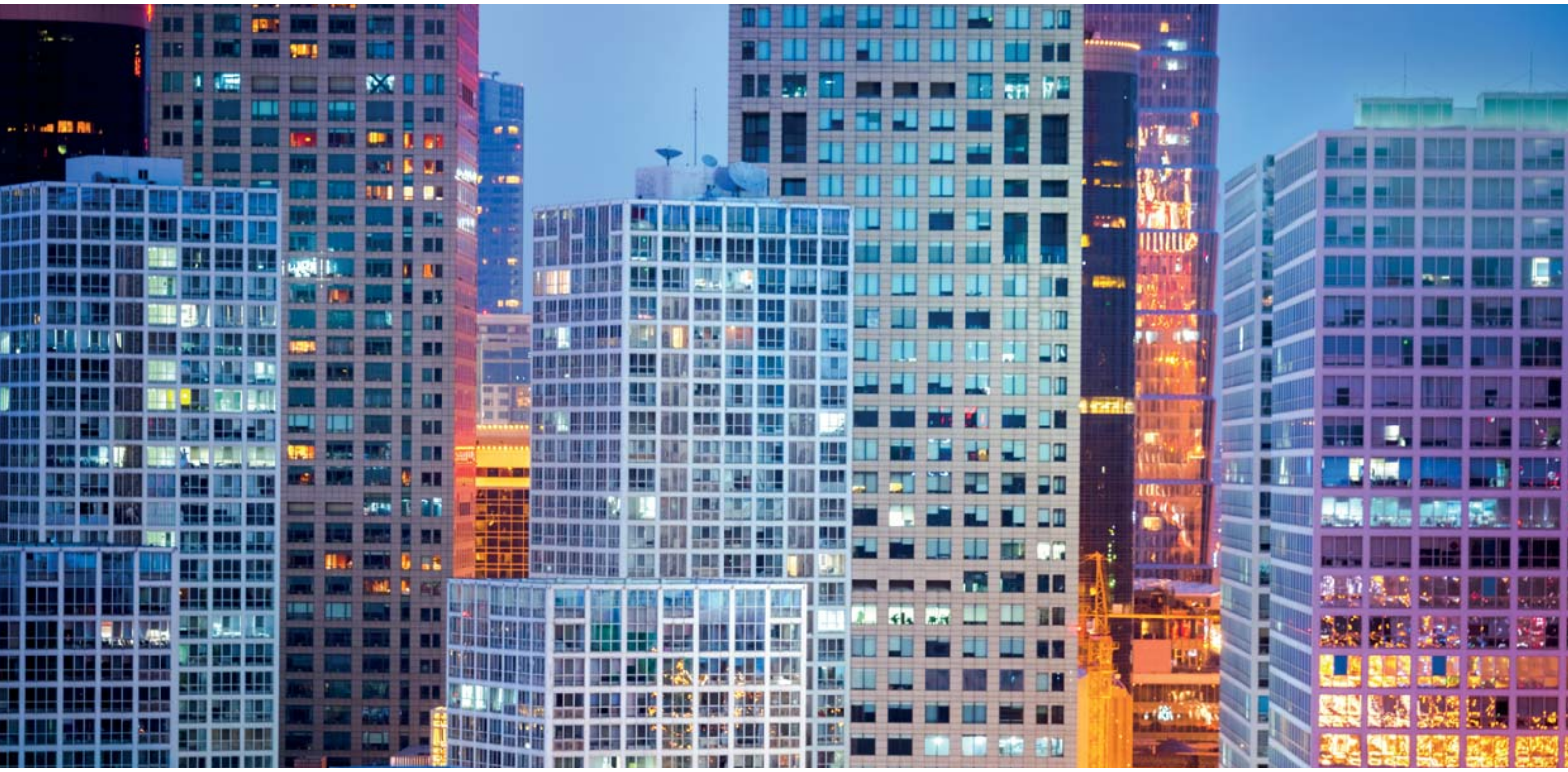
**36%**

Incidence rate of Business Misconduct, the highest in East Africa an indication of a likely gap in business ethics

**Asset Misappropriation in 2018**




***The prevalence rate of Asset Misappropriation in Uganda is significantly lower than the East Africa, Africa and global averages***



Asset misappropriation ranked second in Uganda after Fraud Committed by the Consumer as the most disruptive economic crime over the previous 24 months having been cited by 19% of respondents. It also ties for second place with Fraud Committed by the Consumer at 17%, as the economic crime respondents anticipate to be most disruptive over the next 24 months.

Globally, Asset Misappropriation is perceived as a traditional “brick and mortar” form of crime in a highly advanced technological society. Therefore, it is often overshadowed by other economic crimes that often involve highly sophisticated technological tools, such as Cybercrime.

This does not however seem to be the case in Uganda where 19% of Uganda respondents indicated that Asset Misappropriation was the most disruptive form of economic crime suffered by their organisations in the past 24 months, which is comparable to the 17% of the respondents that indicated that they perceived Asset Misappropriation to be the form of crime most likely to be disruptive to their organisations in the next 24 months.

Against an average incidence rate of 52% for all forms of economic crimes, 75% of the global respondents who cited Asset Misappropriation as the most disruptive form of economic crime in the past 24 months also cited an internal actor as the perpetrator of the fraud. To curb Asset Misappropriation, therefore, it is imperative to invest resources into hiring people with a high level of integrity and accountability. Organisations seeking to recruit the right people must conduct rigorous background checks into the prospective employees' professional and criminal history as well as confirm general conduct with credible references.

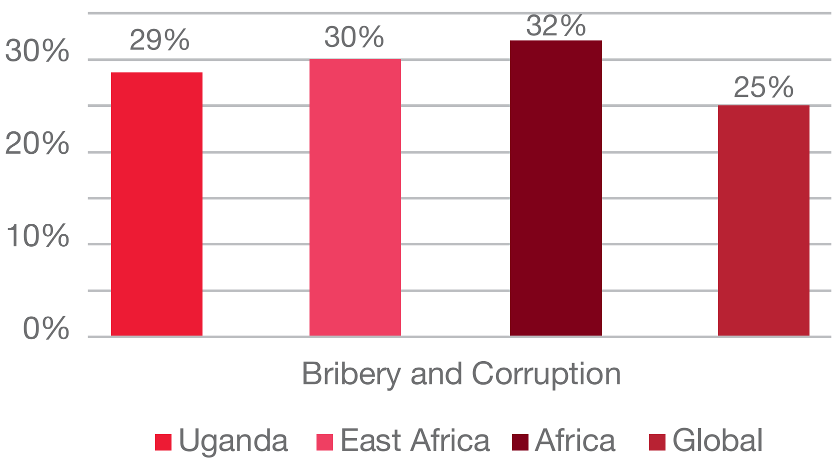
**3 in 4**

respondents that suffered Asset Misappropriation cited an internal actor as having committed the crime, a pointer to the need for enhanced recruitment screening

## Bribery and Corruption

With a 29% incidence rate, Bribery and Corruption is the fifth most prevalent form of economic crime experienced by Ugandan organisations according to the results of the survey. This is against the 30% incidence rate in East Africa, 32% in all of Africa and 25% globally. The proportion of respondents that

**Bribery and Corruption in 2018**



# Africa

Incidences of Bribery and Corruption consistently higher in Africa than in the rest of the world. 3 in 10 Uganda respondents reported having experienced Bribery and Corruption

experienced incidents of Bribery and Corruption is observed to be consistently larger in African countries than in the rest of the world, which puts into the spotlight the vigilance and enforcement of regulations in place to curb the vice.

Bribery and corruption also ranked fifth as the most disruptive economic crime over the previous 24 months with 7% of respondents indicating the same. This is not expected to change with only 3% of respondents indicating that they anticipated it to be the most disruptive economic crime over the next 24 months.

Various legislations have been passed in Uganda aimed at curbing Bribery and Corruption, with the Anti-Corruption Act of 2009 being the most notable. The Act details the kinds of economic crimes that would be subject to the legislation and these include corruption, the bribery of a public official, influence peddling, and diversion of public resources among other actions.

It also allows for the forfeiture or permanent deprivation of corrupt proceeds by order of court after a conviction. In 2010, the Whistleblowers Protection Act was also passed which provided procedures for disclosure of impropriety and protection from victimization and court action.

In the Public Service sector, the Code of Conduct and Ethics of 2005 and the Leadership Code Act of 2002 also regulate certain conduct including receiving gifts and conflicts of interest. As of 2017, there are also relevant drafts of legislation pending in Parliament such as the Proceeds of Corruption Assets Recovery Bill (2013) which is unfortunately not available to the public.

Evidently, the legal and regulatory frameworks exist to effectively deal with Bribery and Corruption in the public sector. The question is why the incidence rate persists at a rather high level.

This could mean that institutions in place lack the necessary will or support to effectively carry out their mandate in accordance with the laws and regulations. Another possible gap is the lack of legislation that specifically tackles Bribery in the private sector. Such legislations have recently been passed in countries like Kenya (2016) and the UK (2012) with notable impact.

## Counting the Cost and Consequences of Economic Crime

Against the global average of 19%, 24% of Uganda's respondents who reported having experienced economic crime indicated that they suffered a direct loss of between USD 100K (c. UGX 351.6M[6]) and USD 1M (c. UGX 3.51B) to the most disruptive crime they experienced in the past 24 months of operations.

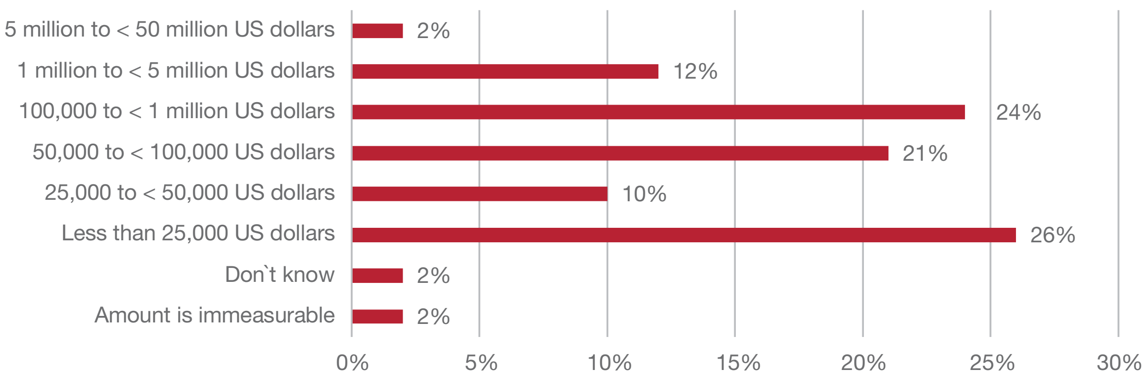
Further, 74% of the survey respondents indicated that they lost at least USD 25,000 (c. UGX 87.9M) to the most disruptive crime they experienced in the past 24 months of operations compared to 63% of respondents who indicated they lost the same amount globally.

Instructively, 2% of the respondents in Uganda indicated they lost more than USD 5M (c. UGX 17.58B) to the most disruptive crime showing just how costly economic crime can be.

# 17B

2% of respondents that suffered economic crime lost 17 Billion shillings or more

**In financial terms, approximately, how much do you think your organisation may have directly lost through the most disruptive crime over the last 24 months?**




[6]1USD = UGX 3516; based on the average of Official Mid-rates for both 2016 and 2017 from the Bank of Uganda

In addition to the direct loss incurred as a result of an economic crime, 46% of our global respondents indicated that they incurred either the same or more cost through the undertaking of investigations and other intervention measures against the recurrence of the crime. This is compared to 24% that was reported in Uganda, only about half of the global proportion. While this could be an indication of efficiency in the undertaking of investigations in Uganda, it could also be an indication that Ugandan organisations need to invest more in the fight against fraud.

Along with these monetary costs, other costs cited as having resulted from the occurrence of the economic crimes include the severing of business relations, brand and reputational damage, the plummeting of employee morale, and strained relations with the regulators. We shall examine some of these effects in the subsequent paragraphs below.

Half of the respondents stated that they thought that the most disruptive economic crime experienced had a medium to high impact on employee morale. This fact demonstrates that organisations acknowledge the steep nonmonetary cost of economic crime on the productivity of their human capital and serves as a cautionary tale to company leadership that does not put in place sufficient measures to rein in this vice.

In an interesting turn, a majority of respondents saw no effect on the share price of their organisation. A similar case can be made on the reputation and brand strength of the organisations in which 60% of respondents saw little to no impact on the brand equity of their firms. Business relations were also considered generally immune to the most disruptive crime experienced by respondents with 62% of respondents reporting little to no impact caused by their most disruptive crime.

Despite the apparent insensitivity of organisations' share price to economic crimes in Uganda, a number of cautionary tales as to the profound effect fraud can have on organisations exist.

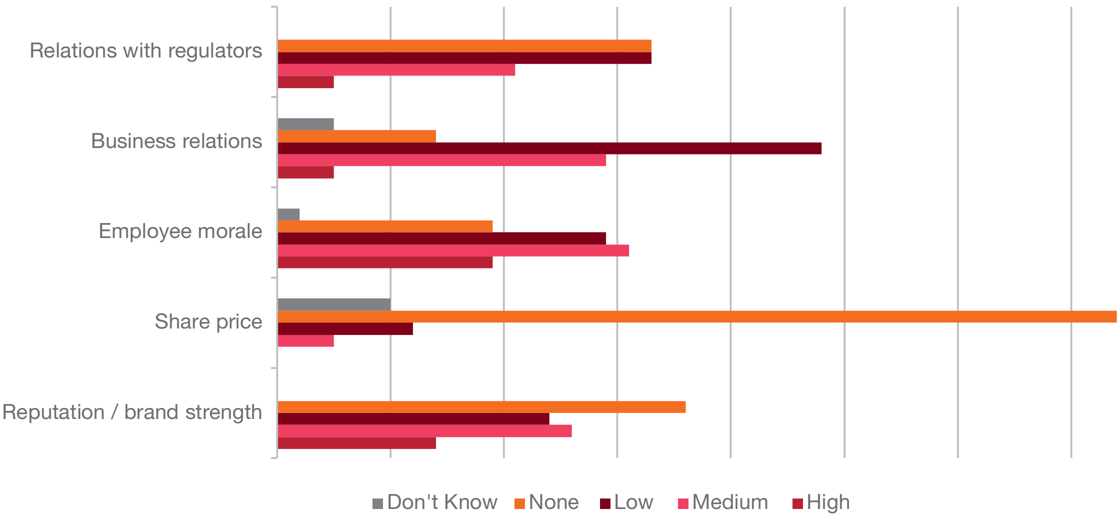
One of the most recent cases involves a multinational furniture retailer in South Africa which announced that it had uncovered accounting irregularities, causing its share price to decline by 80% in the two days following the announcement and wiping out USD 14 billion from their market value.

As such, Whereas the perceived immunity of share prices espoused in the survey may be as a result of inelasticity of the Ugandan market, it is also probable that it may be due to more effective public relations and crisis management infrastructures or, more worryingly, a blissful ignorance of the fraud by key stakeholders including shareholders, customers and the general public.

**24%**

of respondents indicated spending either the same amount or more cost investigating losses from economic crime

**What was the level of impact of the most disruptive crime experienced on the following aspects of your business operations?**




***In addition to monetary losses, organisations also suffered severed business relations, brand and reputational damage, reduced employee morale and strained relations with regulators***

## Profile of the Perpetrator

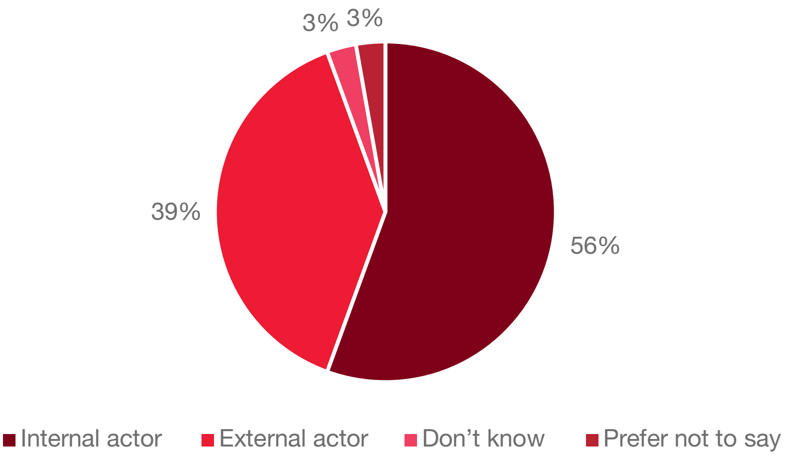
### Internal and External fraud – Enemies within and outside

The most common perpetrator of economic crime identified in Uganda was an internal actor. According to 56% of those surveyed, the economic crime suffered was perpetrated by an internal actor with 39% of respondents identifying an external actor as the perpetrator of the most disruptive economic crime detected.

**56%**

of Uganda perpetrators who suffered an economic crime attributed it to an internal actor

**Profile of the perpetrator**




***Screening of new hires, inculcating an open culture and internal controls can go along way in combatting internal fraud***

### External enemies - Customers!

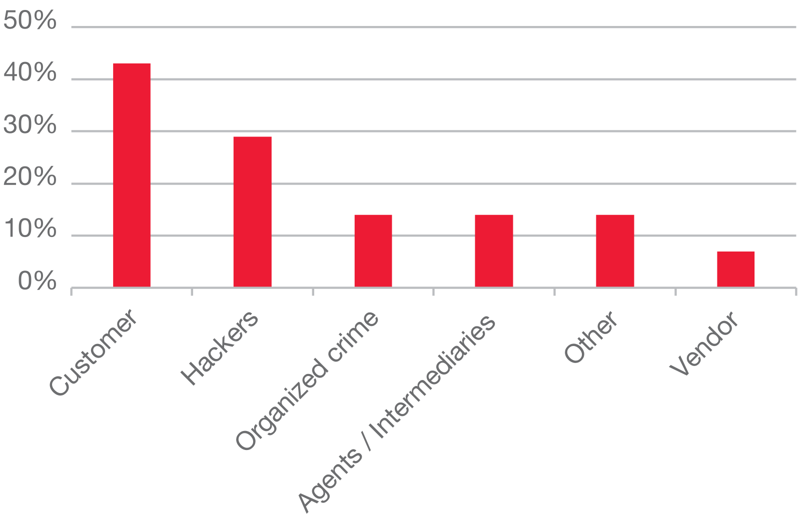
Of the respondents who cited external agents as the main perpetrators of the most disruptive fraud, the top 2 perpetrators were customers and hackers. 43% of Uganda respondents attributed fraud experienced externally to customers with 29% of them singling out hackers as the main external perpetrators.

The eminence of customers as external fraudsters is in tandem with Fraud Committed by the Consumer being the most prevalent form of economic crime in Uganda.

**43%**

of Uganda respondents that suffered crime from external fraud cited customers as the perpetrators

**Who are the main external perpetrators?**




***Customers. hackers and organised crime and agents were cited as the main perpetrators of external fraud***

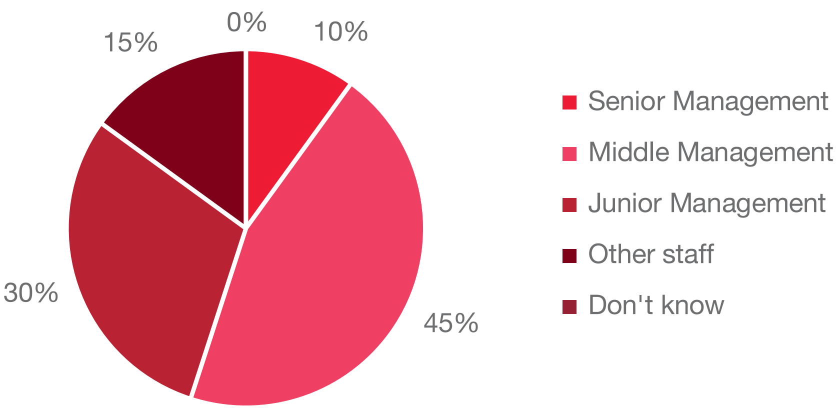
## Enemies within – the internal fraudster

Of the respondents who suffered crime perpetrated by internal agents, 45% indicated that the main perpetrator was in middle level management with junior and senior management being cited by 30% and 10% of respondents respectively.

**3 in 4**

of the internal fraudsters were either junior or middle management

**Rank of the Internal Fraudster**




***Globally the share of serious internal fraud committed by senior management globally continues to rise dramatically - up 50% from 2016***

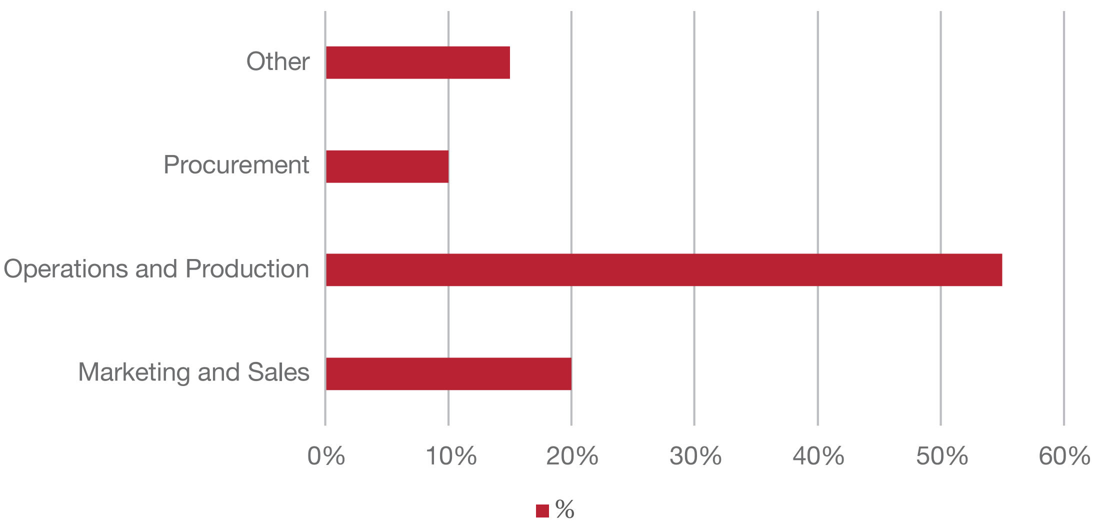
55% of the respondents indicated that the principle function under which the main internal perpetrator resided was Operations and Productions. Marketing and Sales (20%) and Procurement (10%) were the other two functions within which the internal perpetrator was most likely to reside.

It is thus paramount that organisations tighten controls around the production cycle to combat fraud perpetrated by insiders.

**55%**

of internal perpetrators resided in the operations and production functions

**Function of the Internal Fraudster**



# Customer – your friend and foe

*Customers aren't just one consideration of your business – they are your business*

At an incidence rate of 45%, our survey found that Fraud Committed by the Consumer is the most prevalent type of economic crime experienced by Ugandan organisations. It is also the second most prevalent economic crime in East Africa, Africa and globally. Additionally, customers were reported as the most likely outsider to perpetrate fraud. We therefore in this section discuss the consumer and the fraud risk that they portend.

## A rising threat? – Why fraud from consumers in increasing

There are many reasons and circumstances that all work in concert to result in an increased threat from the consumer. We explore only a few here.

### Changing demands of the consumer

The first factor we explore is the changing demands of the consumer. With the ubiquity of technology today, the 21st Century consumer has become used to convenience and on-demand service. This consumer wants to spend the least amount of time and effort while being served. Organisations from banks to governments have thus been forced to adopt new technologies that make them more accessible and efficient.

In the process, we have for instance witnessed a shift from tellers and bank branches to mobile money agents and banking services on mobile applications. These technological advances, however, come with a number of threats arising both from the organisation's unfamiliarity with the technology and the added access that the consumer gets to the organisation through the technological channel linking the two.

### Loss of valuable permanent staff

Another consequence of the enhanced technological uptake is the reduction of permanent staff and their replacement either by the technology itself or by outsourced third parties. Organisations have taken advantage of the technological advances to downsize or to introduce agents who are cheaper to maintain and increase the organisations' reach at minimal cost.

Consequently, the trusted employee that is well versed in an organisation's culture and values is increasingly not the main point of contact between the consumer and the organisation.

### Multiple product packages that are poorly understood

The rapid change in trends and entry of market disruptors have also seen organisations that have traditionally offered a singular service chart into new offerings. These organisations find themselves in environments where they often have limited experience and know-how of the associated fraud risks and regulatory frameworks. As banks offer insurance products and manufacturers get into real estate, they all find themselves in unfamiliar territory that is fraught with danger.

### Changes in lifestyle trends

Finally, in societies where the cost of living is increasing, lifestyle trends promote more consumerism and traditional values are discarded, the consumer—just like the employee—is under more pressure to commit fraud. Consumers also find it easier to rationalize fraud whether the fraud is a failure to pay a public utility or it is a case of shoplifting.

**45%**

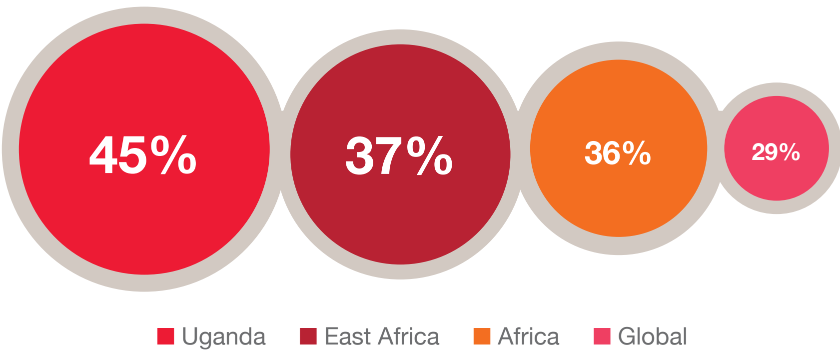
Fraud Committed by the Consumer was the most prevalent type of crime in Uganda and the highest rate in Africa

## Industry and Regional analyses

As indicated above, at an incidence rate of 45%, Fraud Committed by the Consumer is the most prevalent type of economic crime experienced by Ugandan organisations followed by Business Conduct/Misconduct. This is 16% more than the reported prevalence globally.

At 21%, it is also considered by the highest number of respondents as the most disruptive type of economic crime in their organisations over the past 24 months of the survey followed by Asset Misappropriation at 19%. The prevalence of Fraud Committed by the Consumer is also reflected in the East Africa region where it is the second most prevalent form of economic crime at 37% only behind Asset Misappropriation at 46%.

**Fraud Committed by the Consumer**



# KYC

Are your customers who they say they are? Have you profiled them sufficiently?

Fraud by the consumer is especially prevalent in the Financial Services sector where it also had the highest incidence rate at 57% ahead of Cybercrime at 39% and Asset Misappropriation at 29%.

The survey indicates that financial institutions such as banks are a major target of fraud by the consumers, where the consumers exploit loopholes in the designing of financial products or instruments to perpetrate fraud. In East Africa, Fraud Committed by the Consumer has an incidence rate of 62% in the Financial Services sector again followed by Cybercrime and Asset Misappropriation at 44% and 35% respectively.

Whereas our survey results show that on average Fraud Committed by the Consumer is less prevalent in other sectors, from our experience a sizeable number of organisations in other industries are grappling with Fraud Committed by Consumers such as non-payment for goods and services and more complex frauds involving cybercrime or collusion with internal parties.

## Detection and prevention of Fraud Committed by the Consumer

### Know your customer/consumer protocols

The Know Your Consumer/Customer ("KYC") protocols are mechanisms employed by an organisations to identify and verify the identity of a prospective customer prior to making an engagement with them as well as to ensure the organisation becomes aware of any changes to the consumer's identity subsequent to the first engagement.

To successfully avert and detect fraud, the customer acceptance and on-boarding procedures of the organisation must be rigorous enough to ensure that the organisation only engages organisations and persons that are who they say they are.

Organisations must seek to examine the full profile of the prospective customer including any criminal history, type of activities undertaken by the consumer, any ethical or legal non-compliance history and general brand profile.

Customer Acceptance Procedures must also encompass the verification and validation of documents presented by the prospective client including identification documents, documents evidencing ownership of assets, registration documents etc. Whereas Customer Acceptance Policies are not an end in themselves and are unlikely to curb fraud perpetrated by legitimate customers who subsequently identify loopholes for fraud, they can help to single out suspicious persons, imposters or abnormal transactions.

In undertaking these KYC procedures, however, a fine balance must be struck between remaining vigilant and conveying the perception of suspicion towards potential consumers.

### Risk Management Procedures

Depending on the scale and volume of an organisation's transactions with consumers, risk management encompasses many activities. One of the main ways organisations can monitor and manage fraudulent activities initiated by their consumers is by creating risk profiles for each existing consumer.

Based on purchasing and payment patterns, an organisation can create a risk profile for individual consumers that will provide guidance on the level of vigilance that is to be employed while dealing with the consumer. For instance, consumers with a propensity to lodge special requests that involve a bypass of an organisation's protocols may be considered to be of a higher risk than those who comply with an organisation's policies.

Other factors to consider are methods of payment, credit period, use of proxies etc. The identity of the consumer is also key to the creation of a risk profile. By their very identity, politically exposed persons (PEPs) warrant keener monitoring. Due to their high level of visibility and influence in the society, PEPs are widely considered to be more susceptible to being victims, conduits or perpetrators of economic crimes especially in areas of Bribery and Corruption, Procurement Fraud and Anti-Money Laundering activities.

# Cybercrime – the crime of the future

**31%**

of respondents who suffered incidents of economic crime suffered cybercrime

Cybercrime, simply defined, is any criminal offense committed by or facilitated through the use of a computer, a digital device or the internet. It includes the distribution of viruses and malware, phishing and pharming, theft of personal information and illegal download of files, among others. As systems continue to become more complex and connected, the threats of cybercrime increase. This requires organisations to understand and be aware of the various kinds of cybercrime threats that they potentially face.

Whereas Cybercrime has only the third highest incidence rate in Uganda at 31% (tying with Asset Misappropriation), it continues to be one of the biggest potential threats to organisations in the future. At 30%, Cybercrime scored the highest among Uganda's respondents as the form of economic crime likely to be most disruptive to their organisations in the next 24 months, both monetarily and otherwise. This perception is also reflected globally where cybercrime is again ranked first at 26% followed by Bribery and Corruption at 12% and Asset misappropriation at 11%.

Of the respondents in Uganda who cited having suffered from Cybercrime in the last 24 months, Malware and Phishing were the most common tools through which Cybercrime was perpetrated in their organisations at a 39% and 31% incidence rate respectively as shown in the graph below:

or places malicious software in the organisation's environment through a benign looking link or file.

## Regulatory environment and collaboration with Law Enforcement

The Electronic Transactions Act of 2011 was enacted to provide a legal and regulatory framework for, among other things, developing a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions.

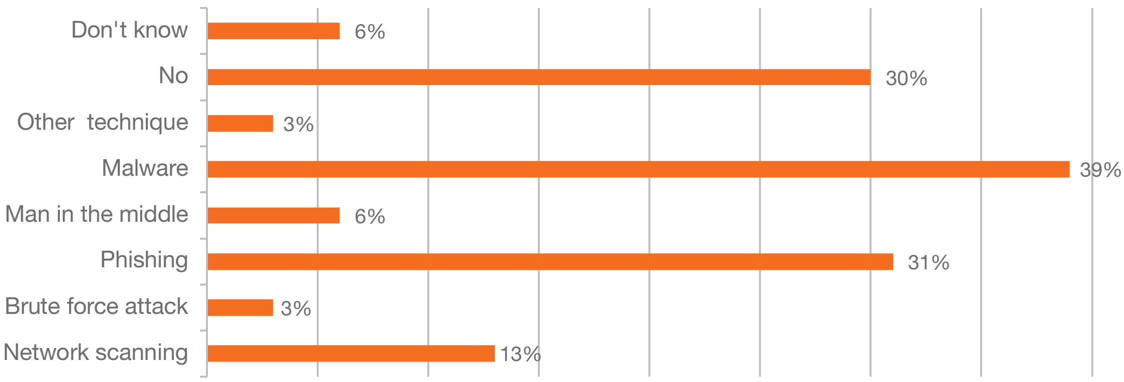
The Computer Misuse Act of 2011 set out to make provision for the safety and security of electronic transactions and information systems, to prevent unlawful access, abuse or misuse of information systems and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment.

The National Information Security Policy (2014) places the burden of information security in an organisation squarely on the Board, requiring them to issue a policy statement that recognizes information as a vital business asset and the management of risks integral to proper corporate governance.

Further to this, the expectation is that the Board

***1 in 3 of cyber-attacks were either Malware or Phishing attacks***

**In the last 24 months, has your organisation been targeted by cyber-attacks using any of the following techniques?**




Malware can be defined as any form of malicious software that infects an organisation's network, servers, devices or end user computers. They include ransomware, remote access tools, network sniffing software and botnet software. Phishing, on the other hand, refers to communications via email, SMS, telephone etc. that seeks information

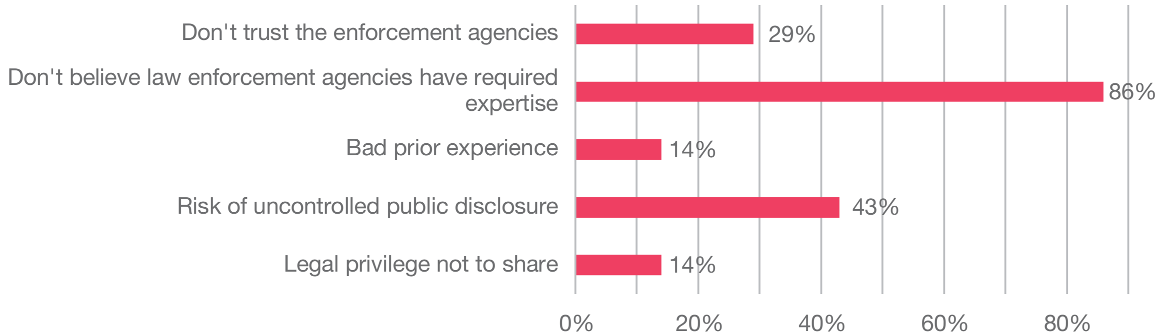
will set a clear strategy for managing risks and that responsibilities are clearly assigned to the management and employees. Based on the narrative and policy documents above, it is clear that cyber-security is considered by the Government of Uganda as a key issue and that it is a priority for heads of organisations as well.

As far as collaborating with law enforcement is concerned, 80% of respondents in Uganda said that they are either likely or very likely to share information with government/law enforcement agencies about suspicion of or subjection to cyberattacks whereas 7% said they are either unlikely or very unlikely to share the same information.

Of the minority of respondents who said that they are unlikely to report suspicion of Cybercrime, the top two reasons given were a lack of confidence in the law enforcement agencies' expertise in handling Cybercrime incidents and the risk of uncontrolled public disclosure.

The Government of Uganda therefore has a responsibility to enhance public trust in the expertise and confidentiality of law enforcement agencies. This can be done through rigorous training exercises with the participation of both public and private entities.

**You stated that your organisation would be unlikely to share information with government / law enforcement agencies about suspicion of or subjection to cyber-attacks. What are the reasons that would make this unlikely?**



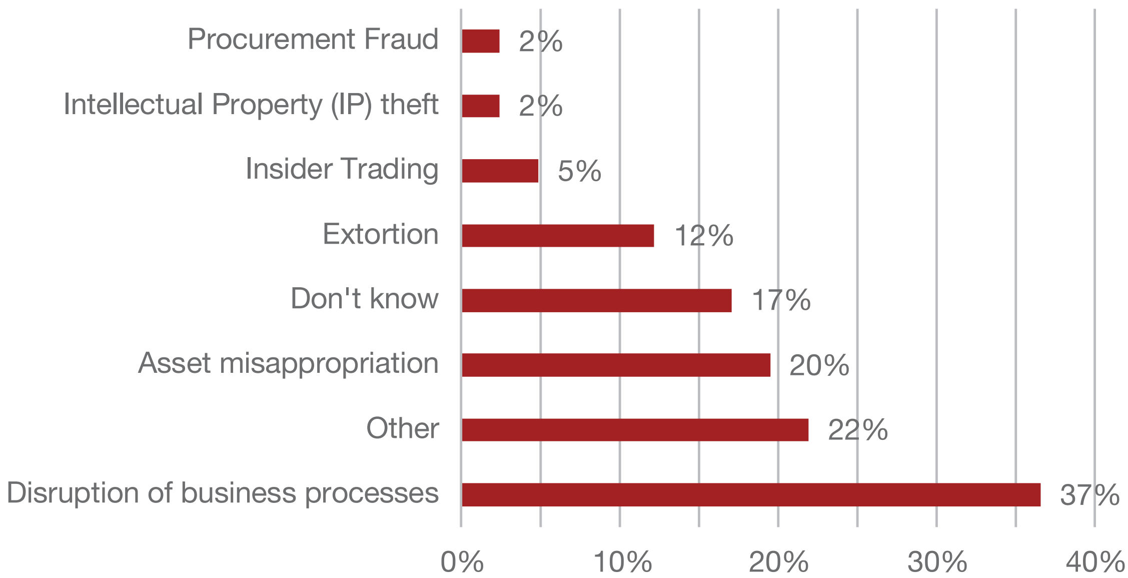

**7%**

of the respondents said they were unlikely to share information on cyber attacks with law enforcement. A small but still worrying percentage

## Effects of Cybercrime

Both in monetary terms and otherwise, the effects of Cybercrime are often catastrophic to many organisations. A Cybercrime attack often results in loss of funds, disruption of business processes and increased regulatory scrutiny on top of loss of consumer confidence. Going by the results of the survey, the most common consequence of a cyber-attack, according to 37% of respondents, was the disruption of business processes followed by asset misappropriation. This is not surprising given the increasing reliance by firms on information systems and software for managing business processes.

**Economic Crime as a result of a cyber attack**



## Defensive strategy

We note that 78% of our respondents reported to have a cyber-security programme that is fully in operation compared to 59% globally and 61% in the East African region. The data thus renders itself to contrasting interpretations. On the one hand, we might be seeing a corporate environment in which firms are acutely aware of the importance of cyber-security evidenced by the programs put in place by 78% of respondents.

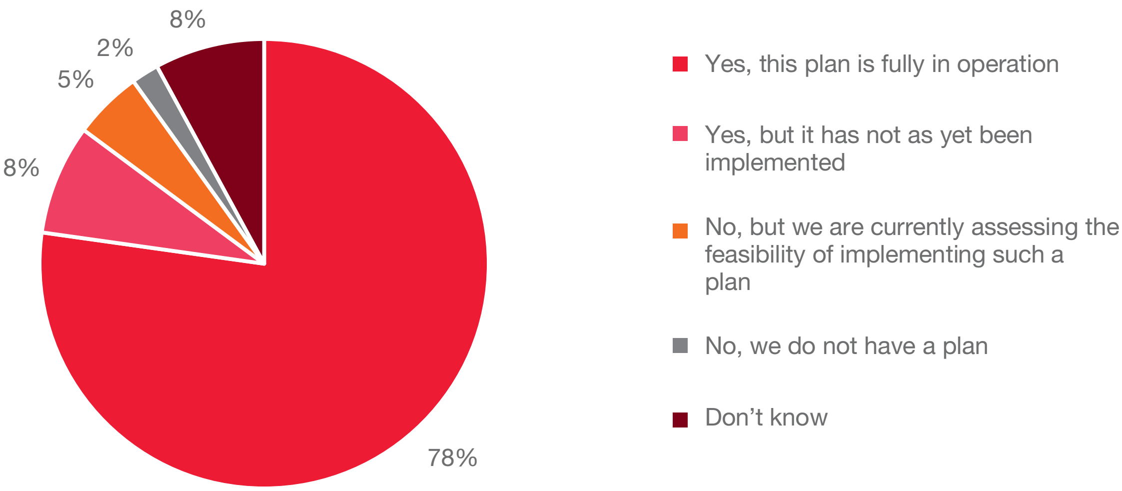
On the other hand, we might be observing from the respondents an overconfidence in the robustness of their cyber-security programs which could indicate an incautious and complacent approach. Either way, it is an encouraging sign to observe that cybersecurity is top of mind for more than half of the organisations surveyed across the board.

The same technology that allows cybercrime can also be marshalled to defend against the crime. As criminals become more sophisticated, so must the tools used to detect and prevent cyber-crime. From the survey, we can see a great awareness of this by the respondents with 83% of respondents either using technology as a primary monitoring technique or part of a wider program of monitoring. This is an encouraging fact which shows that organisations are preparing adequately in the information age.

**78%**

of responses siad they had a fully operational cyber security program, an encouraging statistic

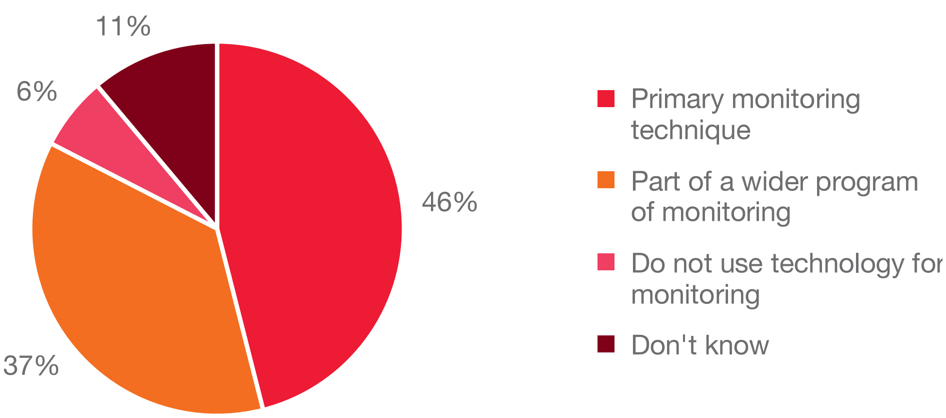
**Does your organisation have a Cyber Security Program (preventative/detective) to deal with cyber-attacks?**




**00%**

Nat vendici mintios aut opta in ni nostist, omnianimin eos anienda sectionest,

**To what extent do you use technology as an instrument to monitor cyber-attacks vulnerabilities?**



# Strengthening the fort – Managing Economic Crime

**15%**

of the respondents reported having limited or no insight into prevalence of economic crime in the organisation, a small but still worrying percentage given the seniority of the respondents

## Blind spots – How to deal with them

*If you don't know it's there, you don't look for it. If you don't look for it, you don't find it. If you don't find it, you can't make the business case to look for it.*

In this survey, 85% of our respondents reported having insight into fraud and/or economic crime incidence in their organisation. This is in line with the Global outlook with 84% of respondents globally reporting the same. Given that successful prevention, detection and management of economic crime primarily depends on the ability of key parties within the organisation to recognize the types of economic crimes, these results are encouraging.

However, 15% of the respondents reported having either limited or no insight at all into the prevalence of economic crimes in their organisation. This means that the organisations are not in a position to institute controls or regulations that may prevent future economic crimes and the occurrence of a fraudulent activity may go undetected. Boards and senior management of organisations must stay accountable and informed on what is going on in their organisations.

## Sniffing out crime – Controls as the weapon of choice

The survey reveals that in order to detect and manage fraud dynamically, all the facets of fraud detection must be carefully examined. Not only is it necessary to have the right technology and internal controls in place, organisations must invest in people and create an organisation culture where integrity, transparency, vigilance and accountability are encouraged and upheld by all stakeholders.

Against a global average of 51%, 61% of our Uganda respondents cited corporate controls as the means by which their most disruptive economic crime was detected. Fraud risk management exercises, suspicious activity monitoring and routine internal audits were cited as the top three corporate control tools employed by respondents and which were capable of detecting the perpetration of economic crimes.

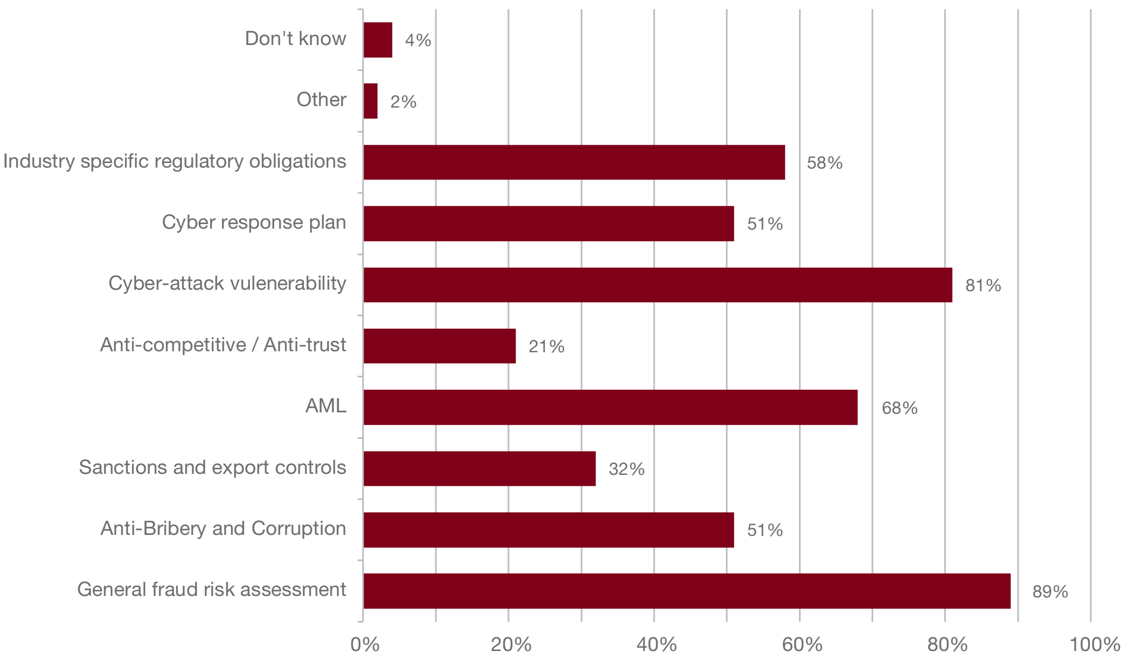
Other corporate controls to detect economic crimes included data analytics, personnel rotation and having in place a robust physical and Information Technology security systems.

For a majority of respondents, risk assessments were carried out with a focus on general fraud risk assessments, cybersecurity and anti-money laundering. Moving forward, organisations will need to leverage on and harness data generated in the course of normal business operations to detect and fight fraud.

By employing data analytics tools and models to make sense of large and unstructured transaction data sets, an organisation can gather useful insights on transaction anomalies, patterns and relationships that may indicate irregular or fraudulent activities.

***Data analytics can be a useful tool in making sense out of large and unstructured transaction data sets***

**In the last 24 months, has your organisation performed a risk assessment on any of the following areas?**



## The human touch – investing in people

Compared to a global average of 27%, 19% of Ugandan respondents cited an open corporate culture as a key means through which their most disruptive fraud activities were initially detected. Respondents indicated that having internal/external tip offs as wells as whistleblowing hotlines helped in the initial detection of suspicious activities. This goes to show that cultivating a corporate culture where internal parties are well trained to identify fraud and feel safe to report fraudulent activities is paramount to the fight against economic crime. A whistle-blower policy that not only encourages the reporting of suspicious activities but also protects the identities and welfare of the whistle-blowers also goes a long way to earn the confidence of potential whistle-blowers.

## Wildcard crimes – detection beyond the grasp of management

9% of our respondents indicated that their most disruptive economic crimes were detected beyond the influences of management, either by accident, by law enforcement or as part of investigative media journalism. Fraud detection that is not under the grasp of the organisation's management runs the risk of damaging the reputation and brand of the organisation. The stream of information being released to the public with respect to the fraud is likely to be uncontrolled, misleading or distorted which provides an opportunity for competitors and other ill-intentioned adversaries to take advantage of the fraud to cause further disrepute to the organisation. As such, the organisation's management should endeavour to ensure that systems in place are sufficient to detect any fraudulent activity before it is in the public domain.

## Prevention of economic crimes

### The sweet spot – the right technology for the right crime

In an age of emerging technologies that can be exploited to perpetrate crime, organisations need to be vigilant and conduct an in-depth assessment of the right technology to serve the requirements of the organisation taking into account factors such as the size of the organisation and the type and volume of transactions undertaken by the organisation.

The continuous, periodic and proactive monitoring and analysis of organisation's systems including transactions and communications (emails and other organisation communication tools) for patterns and anomalies will continue being useful for the prevention and curbing of many emerging fraud activities.

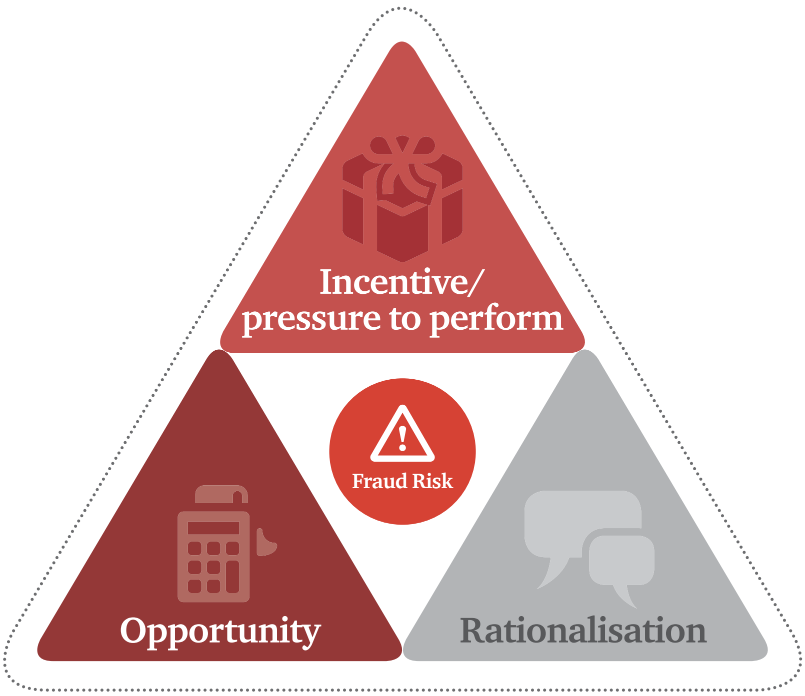
The use of artificial intelligence tools such as speech recognition and machine learning software will also help to arrest economic crimes. Machine learning to curb fraud relies on system interactions with its users to discern user behaviour and the types of transactions that fall within the realm of normal. That way, machines are able to flag behaviour that is indicative of an anomaly and forward the flagged transactions to the relevant authorities for further checking and validation.

### Controls and culture – the fraud triangle

The Fraud Triangle is a powerful method of understanding and measuring the drivers of internal fraud. According to the theory of the Fraud Triangle, the birth of a fraudulent act usually takes the following trajectory.

First, it starts with pressure which is generally related to an internal issue in the organisation or a personal matter the individual is grappling with. Then, if an opportunity presents itself, the person will usually wrestle with it psychologically. The last piece of the puzzle which enables them to move from thought to action is rationalisation. Since all three drivers must be present for an act of fraud to occur, all three must be addressed individually, in ways that are both appropriate and effective.

*An open corporate culture is a key means through which fraud can be detected*



## The antidote to pressure-openness

Corporate-sized frauds are often connected to corporate pressures including unreasonable targets and job insecurity. These pressures can arise at any level of the organisation. Besides corporate pressures, employees may also face personal and social pressures including maintaining or improving their financial standing amongst peers, family financial difficulties, addictions and lack of a spending discipline.

To address these pressures, organisations need to create an environment where employees' financial and psychological welfare is and is perceived to be a priority. Organisations need to go beyond the financial incentives and address the fear and motivations creating these pressures.

Short-term bespoke controls can serve as a check on whether aggressive performance expectations are leading to fraudulent or illegal behaviour. A well-publicized open door or hotline policy can also help not only as a requisite pressure-release valve, but also as an early warning system for potential problems.

## The antidote to opportunity-controls

Opportunity is the second facet of the fraud triangle and often occurs when an employee identifies a control or enforcement gap in the organisation and in which they perceive that a fraudulent activity is not likely to be detected or connected to them.

Some of the things in the organisation that could lead to an opportunity for fraud include a lack of segregation of duties especially in middle management, lack of policies guiding key processes and lax enforcement on existing policies. Ugandan respondents perceive opportunity as the greatest contributor to the execution of a fraudulent activity with 75% ranking it first among the drivers of fraud.

## The antidote to rationalization- culture

While pressure and opportunity can be influenced and controlled by the organisation to some extent, the element of rationalization is only in the control of the perpetrator. Rationalisation involves the perpetrator of the fraud reconciling the fraudulent act against their own personal code of ethics and their feelings about the act they intend to commit.

The first step to providing an antithesis to rationalization is to focus on the environment that governs employee behaviour. Surveys, focus groups and in-depth interviews can assess the organisation's cultural strengths and weaknesses and identify areas that are lax or problematic. Consistent training is also key for employees and other parties to understand what constitutes acceptable behaviour and the consequence of such actions.

# Economic Crime – The East African Perspective

**62%**
the reported prevalence rate of economic crime in East Africa

## Prevalence of economic crimes

In this section, we compare the Uganda results against those of other Eastern Africa countries and in particular Tanzania, Kenya, Rwanda and Zambia.

Whereas we have had country specific reports and statistics in Kenya since 2009 and Zambia since 2014, it is the first time that we have had enough responses to generate reports from Uganda, Tanzania, and Rwanda and this is therefore the first time we are having an East African analysis.

Against the global rate of 49%, the East African region reported an average of 62% prevalence of economic crimes in the last 24 months, with Kenyan respondents reporting the highest prevalence rate at 75% and Rwanda the lowest at 47%.

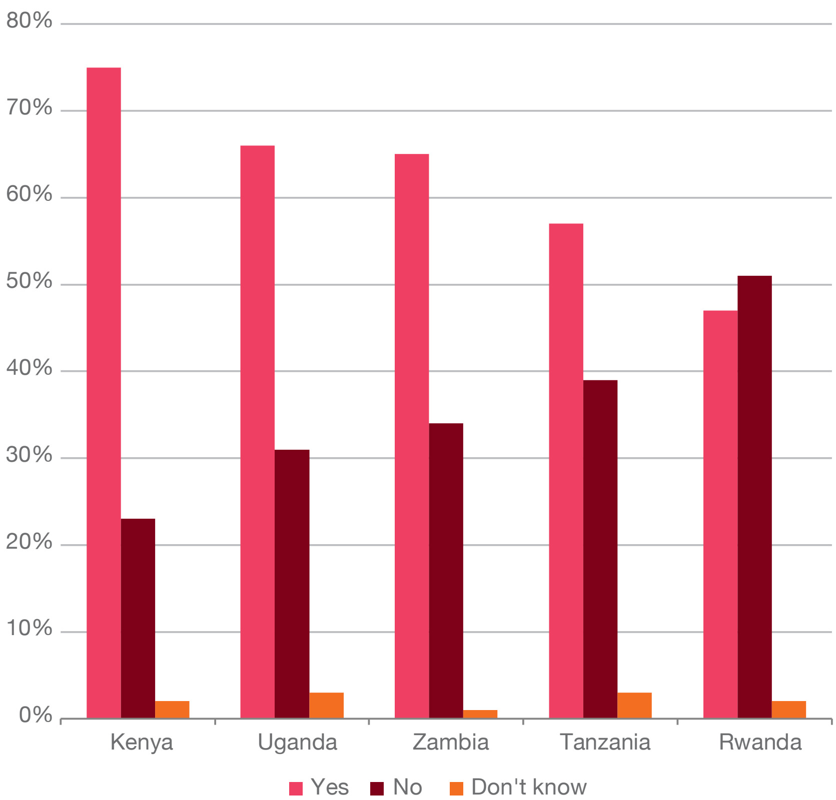
In both Kenya and Zambia, the incidence of economic crimes is higher in 2018 compared to the years 2014 and 2016. As evidenced by this survey, the increase in incidence of economic crimes is a regional and global problem and while each country must put measures to curb the vices at home, there must also be cross-border cooperation in formulating and implementing policies that help prevent, detect and mitigate against various forms of economic crimes.

## Types of economic crimes experienced in East Africa

On average, the top four forms of economic crimes experienced in East Africa were Asset Misappropriation (45%), Fraud Committed by the Consumer (36%), Bribery and Corruption (30%) and Business Conduct/Misconduct (29%).

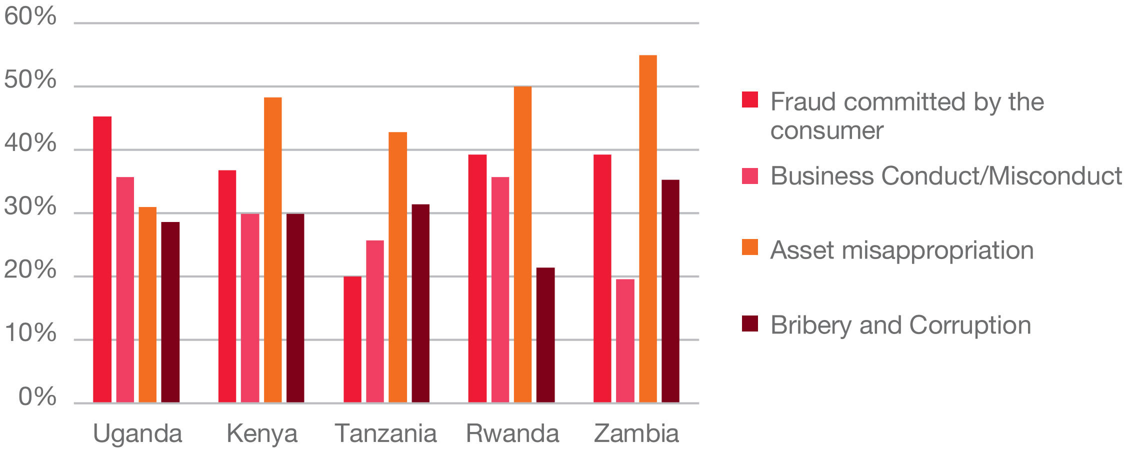
**28%**
the difference between the highest incidence rate reported in East Africa (Kenya at 75%) and the lowest (Rwanda at 47%)

**Prevalence of Economic Crime in East Africa**




***This is the first time since the inception of GECS that we are able to analyse the results from five Eastern Africa countries***

**What types of fraud and/ or economic crime has your organisation experienced within the last 24 months?**




***At 36% the incidence rate of Business Misconduct in Uganda is 24% higher than the East African rate***

As shown in the chart above, different forms of economic crimes are experienced differently in the East African region. In Uganda, the most prevalent form of economic crime is observed to be Fraud Committed by the Consumer at 45% followed by Business Conduct/Misconduct at 36% with the latter being well above the regional average of 29%.

However, as a positive sign in the region, asset misappropriation is lowest in Uganda, at 31%. Zambia takes the lead as the country with the highest prevalence rate for two major economic crimes experienced in the Eastern Africa region which are Asset Misappropriation and Bribery and Corruption. With the exception of Uganda, Asset Misappropriation leads the way as the most prevalent economic crime in East Africa.

Rwanda has the lowest incidence rate of Bribery and Corruption compared to other countries in the region, which may be a testament to the well-known zero-tolerance policy on this form of economic crime in Rwanda. Ranked among the least corrupt countries in various surveys, this status has acted as a key incentive for foreign investment in Rwanda.

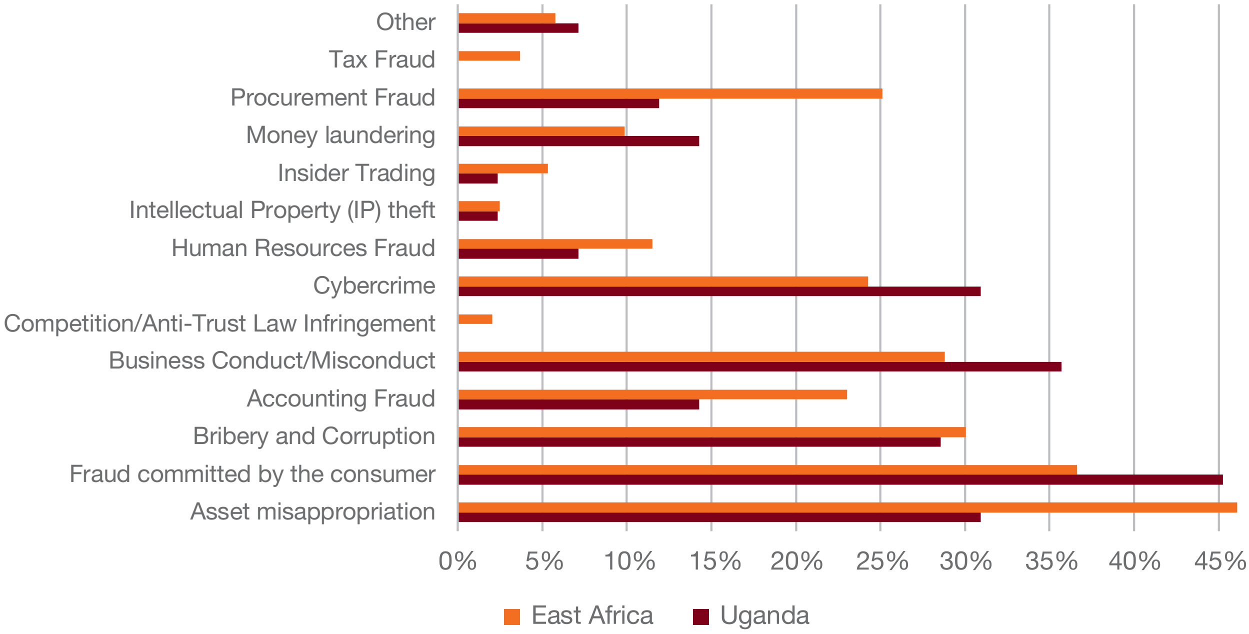
Comparing incidence rates of economic crime in Uganda with those in East Africa, Fraud Committed by the Consumer, Business Conduct/Misconduct and Cybercrime have higher incidence rates in Uganda in comparison to the region. Secondly, for the majority of economic crimes, incidence rates are lower in Uganda when compared with the region at large. They include asset misappropriation, bribery and corruption, accounting fraud, human resources fraud, intellectual property theft, insider trading and procurement fraud.

Some questions that come to the surface with regard to these preliminary observations include why the level of procurement fraud in Uganda is half that in the East African region. Our experience in the region would seem to indicate that this low incidence relative to East Africa may be due to Procurement Fraud happening but going undetected.

This particular hypothesis would apply to Accounting Fraud as well, with an incidence rate that is lower in Uganda compared to rates in the rest of East Africa. If true, this would speak to a lack of effective monitoring mechanisms for this particular type of economic crime and should lead to a re-evaluation of corporate controls in place to mitigate against procurement fraud.

***At half the regional rate, the incidence rate of Procurement Fraud in Uganda is significantly lower, is it a question of low rates or poor detection?***

**What types of fraud and/ or economic crime has your organisation experienced within the last 24 months?**




# 24%

of respondents in both Uganda and across East Africa reported losing between USD100K and USD 1M to the most disruptive form of crime in the preceeding 24 months

The financial losses resulting from economic crimes in the East African region closely resemble those of Uganda.

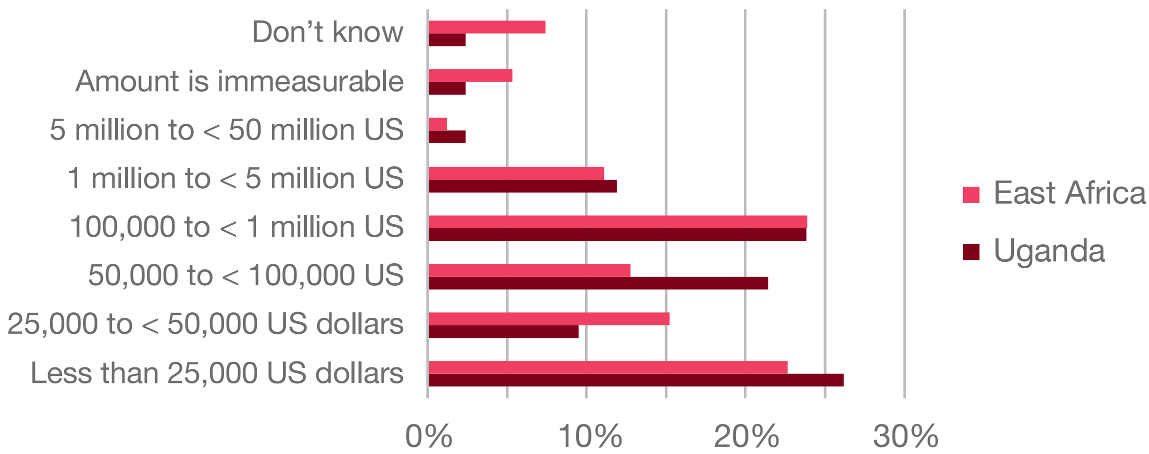
For instance, in Uganda 24% of the respondents reported to have lost between USD 100K and USD 1M to the most disruptive forms of economic crime that they experienced in the past 24 months of operations which is exactly the percentage of East Africa respondents that reported to have lost the same amount.

It would be useful to note that this cost accounting is only financial in nature. The true cost of economic crimes is difficult to quantify.

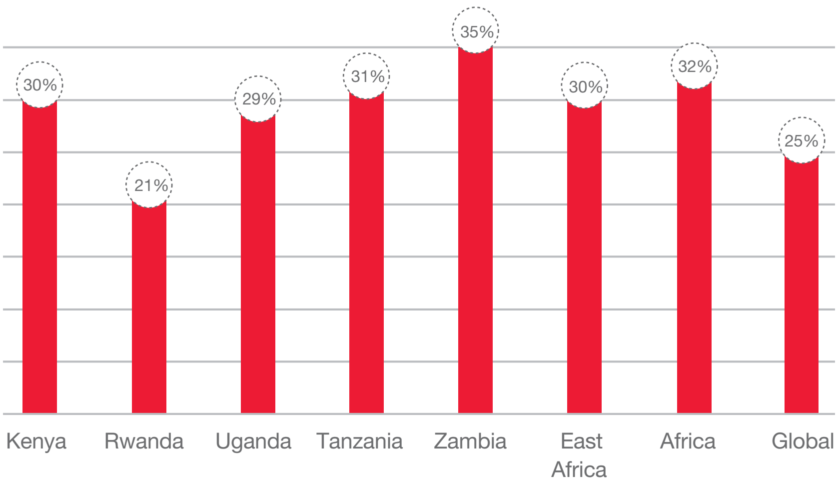
Other factors that have an impact include the loss of employee morale, disruption in business relations, deteriorating relations with the regulators, reputational damage and loss of market value through a drop in share price, most of which are difficult if not impossible to quantify.

With respect to Bribery and Corruption, 30% of the East Africa respondents reported that they experienced this vice in their organisations in the last 24 months, making it the fourth most prevalent form of economic crime. At 35%, Zambia has the highest prevalence of Bribery and Corruption with the least incidence rate being observed in Rwanda at 21%.

**Financial Losses resulting from the most disruptive fraud/economic crime**



**Bribery and Corruption in 2018**




***Economic crime trancends national boundaries necessitating a concerted approach in dealing with it***

In Uganda, 21% of the respondents reported to have been asked to pay a bribe in the last 24 months in their primary country of operations whereas 20% reported that they had lost an opportunity to a competitor who they believed paid a bribe.

Overall, in East Africa, 22% of the respondents reported having been asked to pay a bribe and an equal number reported to have lost an opportunity to a competitor they believe paid a bribe. Bribery and Corruption is a problem that transcends sectoral and regional boundaries. It is therefore critical that all players of the economy converge around creating social and economic accountability mechanisms to curb this vice.

## Compliance and business ethics programmes

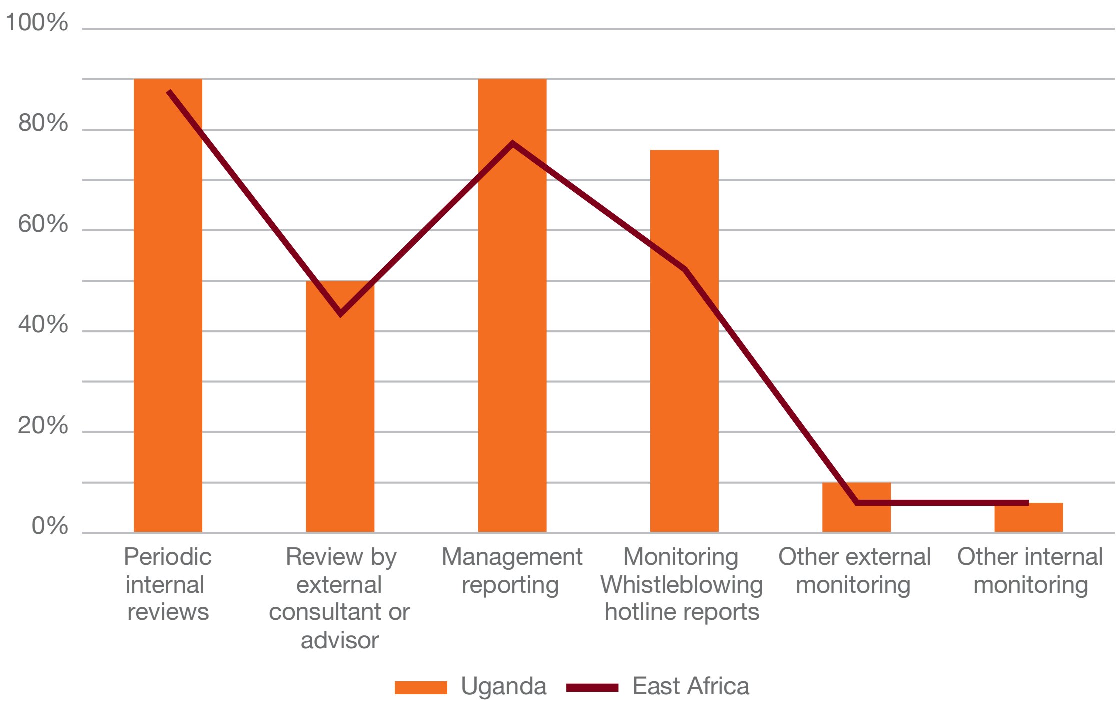
According to the results of the survey, 90% of Uganda and 88% of East Africa respondents indicated that their organisations undertook periodic internal reviews to ensure that compliance and business ethics programs are effective in curbing fraud.

Other key mechanisms reported as being employed to assess the effectiveness of compliance and business ethics programmes include management reporting and monitoring of whistleblowing reports.

50% of Uganda respondents and 44% of East Africa respondents indicated that they used an external consultant or advisor in the monitoring of compliance issues. When compared to the global rate of 38%, we noted that respondents in Uganda and East Africa see greater value in independent third party input as far as the monitoring of compliance issues is concerned.

This is a positive sign since an independent review of an organisation's compliance and ethics programs' effectiveness is necessary to provide an external perspective to areas that may not be familiar to management. Further, since external consultants often report directly to the Board or the senior management team, they are able to break the bureaucratic barriers in the implementation of new ideas.

**How does your organisation ensure that your compliance and business ethics program is effective?**




# Conclusion – what now?

Our survey shows that many organisations are still under-prepared to face fraud, both from internal and external actors. One of the reasons for this could be because many organisations still approach risk management, fraud investigations and reporting as distinctly different functions of the organisation.

Adopting a centralized fraud management framework that is all-encompassing can go a long way in ensuring that fraud prevention is vibrant and detection and investigations are undertaken quickly and effectively. Centralizing these functions not only enhances the efficacy with which information between separate incidents is pieced together and relevant patterns drawn, it also controls for bias that may arise from self-investigation. Further, a holistic approach to fraud management also enables lessons drawn from one function to be applied to other functions within the risk management chain.

While the technological and global revolution of the 21st century demands an investment in machines and modern technology, cultural and human elements of the organisation continue to be a key factor in the detection and management of fraud as demonstrated by the results of this survey.

Organisations must ensure that they have the right people with the right level of integrity and transparency needed to combat and manage fraud. Additionally, a culture of transparency and fraud reporting must be cultivated including implementation of sound policies governing the treatment of tip offs and whistle-blower activities within the organisation.

Advances in technology are essential to the success and sustainability of any modern-day organisation, but it is the people that operate the machines that will keep the interests of the organisation protected and ensure that incidents of fraud are investigated and prosecuted.

Our survey also reinforces the importance of all stakeholders converging in the fight against fraud. While the government must for instance ensure that there is a comprehensive and all-inclusive legal and enforcement framework in place, the private sector, civil society, religious leadership and indeed the entire citizenry must converge around the goal of eradication of economic crimes.

Finally, whereas fraud was seen as a costly nuisance, fighting fraud has progressed from an operational or legal matter to a central business issue. Fraud today is an enterprise that is tech-enabled, innovative, opportunistic and pervasive. It is indeed a formidable competitor that has been overlooked.

# Our comprehensive Forensic Solutions

PwC offers end-to-end active anti-corruption, fraud prevention and investigation solutions to help clients assess fraud; design, implement and maintain a fraud prevention strategy;v and to develop incident response mechanisms.

Our forensics and dispute analysis professionals can robustly assist your organisation by providing a wide variety of advisory services and investigations including:

***Fraud prevention and anti corruption services***

- Fraud risk assessments
- Fraud detection reviews
- Fraud and corruption risk management strategies
- Whistleblowing
- Capacity building in fraud prevention

***Regulatory compliance reviews***

- Compliance with the Kenya Bribery Act
- Compliance with the US Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act
- Compliance with Anti-Money Laundering regulations
- Compliance with other regulations

***Corporate Intelligence***

- Provision of objective, clear and targeted investigative research and analysis
- Better understanding of acquisition targets or business partners e.g. customers, suppliers, agents, licensees
- Intelligence to inform strategic decisions


***Investigations***

- Fraud investigations
- Bribery and corruption
- Asset tracing and recovery
- Litigation support services
- Expert witness services

***Forensic technology solutions***

- Imaging of electronic media
- Data recovery
- Acquiring and analysing computer files
- Cyber crime prevention and response
- Data analytics

***Dispute support services***

- General commercial disputes
- Transaction related disputes
- Intellectual property disputes
- Competition/anti trust disputes
- Capital projects and infrastructure disputes
- Government contract disputes

# Contacts

## Want to know more about what you can do in the fight against fraud? Contact one of our forensics specialists

**Francis Kamulegeya**
Senior Country Partner
+256 312 354 400
francis.kamulegeya@pwc.com

**Muniu Thoithi**
Forensics Leader, Eastern Africa
+254 20 285 5684
muniu.thoithi@pwc.com

**Adam Sengooba**
Associate Director
+256 312 354 400
adam.sengooba@pwc.com

**Uthman Mayanja**
Partner
+256 312 354 400
uthman.mayanja@pwc.com

**John Kamau**
Senior Manager, Kenya
+254 20 285 5065
john.kamau@pwc.com

**Doreen Mugisha**
Manager
+256 312 354 400
doreen.mugisha@pwc.com

## About the survey

PwC's 2018 Global Economic Crime and Fraud Survey was completed by 7,228 respondents in 123 territories. Of the total number of respondents, 52% were senior executives of their respective organisations, 42% represented publicly-listed companies and 55% represented organisations with more than 1000 employees.

In Uganda, the Survey was completed by 64 respondents making Uganda one of the 54 countries that achieved the threshold for a country-specific report. Of the 64 respondents, 48% represented listed companies, 41% private organisations and 11% public or non-governmental organisations.