Fraud: The overlooked competitor

2018 Global Economic Crime and Fraud Survey

TANZANIA REPORT

pwc

www.pwc.com/tz

Foreword

We are pleased to present the first ever Tanzania GECS report

David Tarimo
Country Senior Partner,
PwC Tanzania

Muniu Thoithi
Forensics Leader,
East Africa Region

The Global Economic Crime Survey ("GECS") is a biennial PricewaterhouseCoopers survey that receives and analyses feedback from stakeholders in various economic sectors. In this current survey, the Global Economic Crime Survey 2018 ("GECS 2018"), we received responses from over 7,000 respondents across 123 countries in 18 languages. This makes it one of the largest and most comprehensive surveys on economic crime in the world.

This is the first time that Tanzania has a country specific report having attained the statistical threshold necessary to provide a representative view of the perception of economic crime amongst the Country's survey respondents.

Since our last GECS, which was conducted in October 2015 and launched in February 2016, the world has seen significant changes and events that have helped shape the environment under which the results of this survey can be viewed. The United Kingdom voted in favour of "Brexit" in June 2016. In November of the same 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[1] and is estimated to have grown at 3% in 2017[2].

On the African stage, during the same period, Presidential elections took place in a number of Africa's "market hub" countries, such as Tanzania, Uganda, Rwanda, Zambia, Ghana and Kenya. Election years are usually marked by uncertainty in the markets in most African countries. 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[3] before rising to 2.4% in 2017[4].

Tanzania, one of the fastest growing economies globally, is at a critical point in its development progress. The largest country in the East African region by landmass and blessed with abundant natural resources, from natural gas, precious metals and stones to wildlife and huge tracts of arable land, it has maintained a steady growth in its GDP of about 7% over the last 3 years with activity particularly buoyant in construction, transport and storage, wholesale and retail trade, information and communication and basic manufacturing[5].

Inflation has stabilized at about 5% over the last two years[6]. Tanzania is investing heavily in infrastructure to not only ease movement of people and goods, but also to reduce the cost of doing business in the process. Significant potential infrastructure projects include the US$10bn port at Bagamoyo, the LNG plant in Lindi and the 1,444 crude oil pipeline from Uganda to the Tanzanian coastline. Ongoing significant projects include the construction of a new standard gauge railway line.

It is against this global, pan-African, and Tanzanian backdrop that we release our GECS 2018 report.

At 57% economic crime incidence rate according to the results of the survey, Tanzanian organisation continue to grapple with a relatively high prevalence of economic crimes, although faring better than its East Africa neighbours other than Rwanda. It is notable, however, that the Government of Tanzania has continued to put in place mechanisms to ensure

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

that this prevalence is suppressed in the future. Leading from the front, the President, H.E John Magufuli, has been keen to create an environment of zero tolerance to corruption and other forms of economic crimes in the country.

A shake-up of the Tanzanian Ports Authority and the revenue authorities as well as the much publicized clean-up of the public payroll rooting out ghost workers and civil servants who had faked academic certificates are examples of the intent to clear out corruption and to restrict any loopholes that would create an environment for economic crime to thrive.

In this first ever Tanzania GECS country report, we take a look at some of the forms of economic crime that recorded the highest incidence rates in Tanzania including Asset Misappropriation, Bribery and Corruption and Business Misconduct. Given that Cybercrime is seen by the highest proportion of respondents globally as the most disruptive form of economic crime in the next 24 months, we also give it particular attention in this report.

Further, the report also compares the nature and prevalence of economic crimes across East African countries (i.e. Kenya, Tanzania, Uganda, 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.

The GECS is an important tool for measuring the global and local economic crime environment(s). Our Tanzanian report contains some valuable lessons for Tanzanian organisations. The results would suggest that economic crime in Tanzania continues to be a pervasive problem requiring serious, well thought out and even societal interventions to both prevent and control it.

The prevalence rates also suggests – at least in part – an increased awareness of fraud, and that fighting fraud has progressed from an operational or legal matter to a central business issue. As awareness of the pervasiveness of economic crime continues to persist, and Tanzanian organisations set out policies to prevent and control fraud, we can only hope that the number and costliness of fraud incidents will reduce.

[1]World 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]Bank of Tanzania Annual Report 2016/17

[6]Bank of Tanzania Annual Report 2016/17

Contents

Introduction

5

World view of Economic Crime – Putting it into perspective

6

Focus on Cybercrime and Fraud Committed by the Consumer

13

Managing economic crime –creating a formidable defence

19

An East African view of Economic Crime

24

Introduction

7,000
Respondents from 123 countries in 18 languages

61
Respondents in Tanzania and 379 in East Africa

We are pleased to present the ninth biennial GECS Report and the first Tanzania country report. The report aims to provide insights into the economic crime landscape in the country as obtained from various economic stakeholder respondents of the survey conducted in 2017. In a constantly evolving technological environment, the report also aims to provide a view on the detection and preventive measures that organisations can adopt to combat incidents of economic crime.

Globally, the 2018 GECS Survey Report analyses feedback from over 7,000 stakeholders in various economic sectors across 123 countries in 18 languages. This makes it one of the largest and most comprehensive surveys on economic crimes in the world.

In Tanzania, the report draws insights from the experiences, perceptions and knowledge of economic crime from 61 respondents. The 61 respondents constitute senior officers in diverse positions in the organisational hierarchy including but not limited to those in Executive Management, Finance, Audit, Risk Management and other core functions within large, medium and small organisations with some undertaking operations spanning the globe. Of the 61 respondents, 33% represented listed companies, 56% private organisations while the remaining 11% included government/state-owned enterprises and non-governmental organisations.

In the age of globalization, the prevalence, control and effects of economic crimes in Tanzania is to a significant extent affected by the geopolitical and socioeconomic conditions of the regional blocks it inhabits. This report compares the survey results in Tanzania to those observed in the Eastern African Region (consisting of Kenya, Uganda, Tanzania, Rwanda, as well as Zambia), Africa and globally. It is worthwhile to point out that this is the first time that we have obtained sufficient responses for Tanzania, Uganda and Rwanda to enable us produce a representative country reports and the insights gleaned from comparing the trends in the region is profound.

Of the incidences of economic crime experienced, Asset Misappropriation stands out as the most prevalent economic crime experienced by our survey respondents in Tanzania at 43% incidence rate. Asset Misappropriation also had the highest incidence rate in the East African region and globally. The results of the survey showed that Bribery and Corruption was the second most prevalent economic crime in Tanzania with an incidence rate of 31% which is above the global average of 25%.

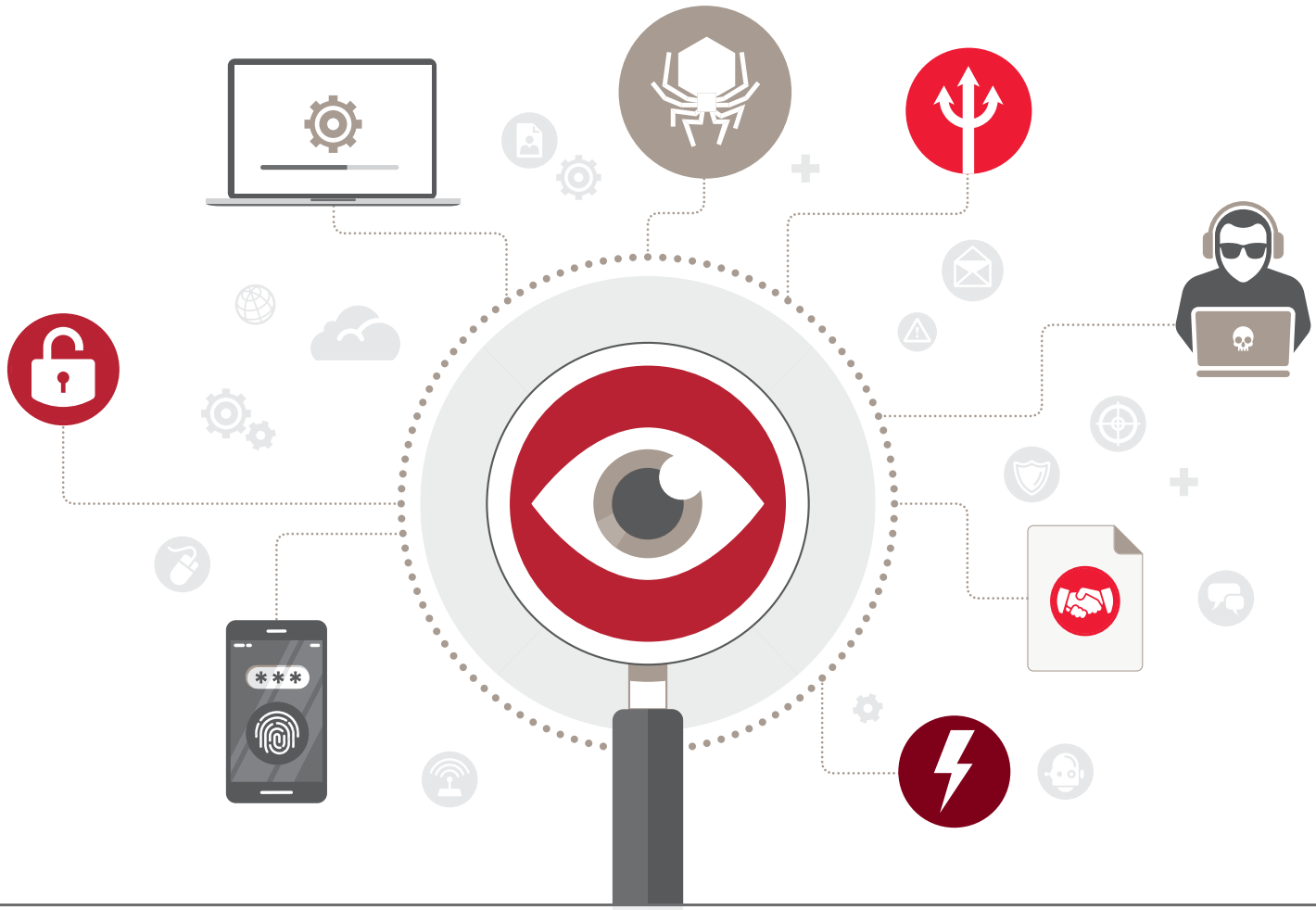
The 2018 Survey included Fraud Committed by the Consumer and Business Misconduct as new economic crime classifications. In Tanzania, Fraud Committed by Consumer turned out to be especially prevalent in the Financial Services industry where it had an incidence rate of 55% becoming the most prevalent form of economic crime, ahead of Cybercrime which has traditionally been the leading form of economic crime in that industry.

In this report, we take a closer look at Fraud Committed by the Consumer and Cybercrime which are amongst the most prevalent economic crimes in the Eastern Africa region and are seen as the crimes of the future.

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 Tanzania respondents as far as detection of economic crimes is concerned.

As far as prevention is concerned, we also 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 what we hope to be useful insights from the same including the need to pay attention to corporate pressures, control and enforcement gaps and the organisational environment and culture.

World view of Economic Crime – Putting it into perspective



57%

of Tanzania respondents reported experiencing economic crime in the preceding two years. This is lower than the East African average of 62% but higher than the global average of 49%

Tanzania versus the World

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. In Tanzania, 57% of our respondents indicated that they had experienced at least one form of economic crime in the last two years.

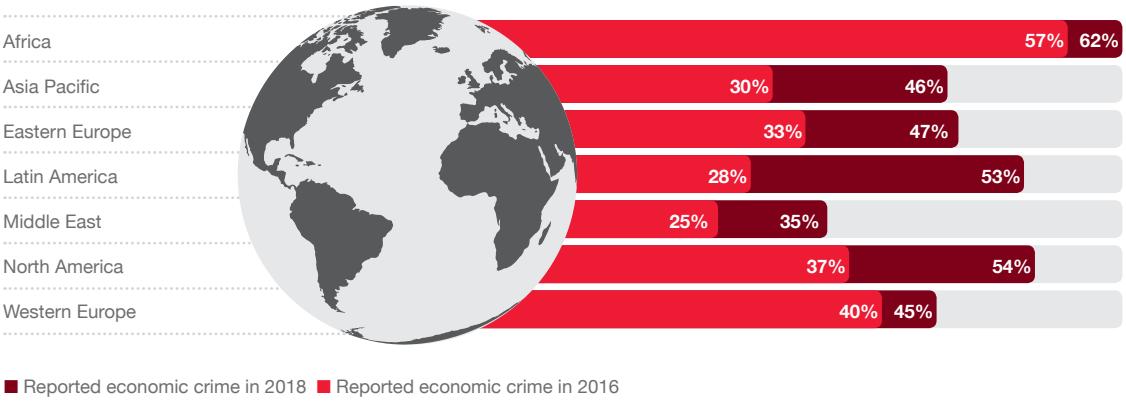
The marked rise in incidences of economic crime is seen to transcend regional blocks. Whereas Africa continues to take the lead in the pervasiveness of economic crimes in the last 24 months at 62% in 2018 up from 57% in 2016, other regions were also not immune to the brunt of the vices.

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% from 2016.

In Africa and globally, the prevalence of economic crimes appear to be at its peak as compared to the survey reports for the last four years. In our assessment, a number of factors could have contributed to this phenomenon including the widening wealth inequality between the rich and the poor, increased connectivity brought about by the ICT revolution coupled with a poor understanding of the controls needed in a highly inter-connected environment and poor enforcement of existing regulations.

Of the 10 countries that reported the highest incidence rates of economic crime globally, we observe that 5 (50%) are African Countries, once again bringing Africa into focus 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



36%
average increase in economic crime

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 fraud practitioners know that the real percentage of economic crime victimisation is significantly higher than the reported incidents — not 49% globally or 57% in Tanzania.

The high rates may therefore be an indicator of a higher awareness of fraud as opposed to a higher incidence. It may also mean that the systems in place are able to identify economic crimes hence the high level of incidents that may have been intercepted or discovered. The reality is more likely therefore that this statistic measures not actual fraud, but

Cost of economic crime is not limited to financial/ monetary loss but includes the cost of investigation, operational time wasted and the general impact on the organisation's reputation

awareness of fraud. Evidently, 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.

Cost of Economic Crimes

In this section we will explore the cost of economic crime which can be viewed as both:- (i) the amount lost to the fraud; (ii) the actual monetary spend channelled towards investigations and other forms of intervention following the economic crime incident; (iii) the operational time wasted as a result of disruption caused by the incident of fraud that is in terms of business operations and shift of the executive management/board's attention towards dealing with the incident of fraud; and (iv) the general impact of the economic crime to the organisation.

Of the respondents that reported to have suffered at least one form of economic crime in Tanzania, 31% reported that they had lost between USD 100K and USD 1M to the most disruptive form of crime.

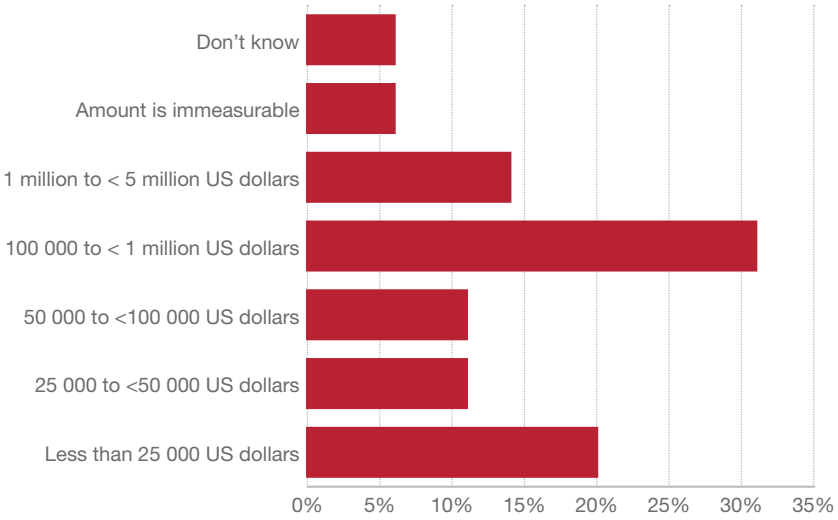
20% reported that they had lost amounts below USD 25K and of significance are the 14% who reported that the amounts lost as a result of the most disruptive form of crime was between USD 1M and USD 5M (between TZS 2.3B – 11.3B).

Asset misappropriation, was cited by the highest number of respondents, 23%, as the most disruptive economic crime noted in Tanzania. This was followed by Cybercrime at 11%.

In Tanzania, the impact of the most disruptive form of economic crime was heavily felt on the reputation/brand strength as well as on the organisations' business relations with 40% of respondents noting these as the most affected aspects of their businesses. The two were followed by employee morale cited by 14% of respondents.

According to the results of the survey, at a 97% response rate, almost all cases of the most disruptive economic crime within organisations in Tanzania were reported to have been brought to the attention of the board/senior leaders in charge of governance.

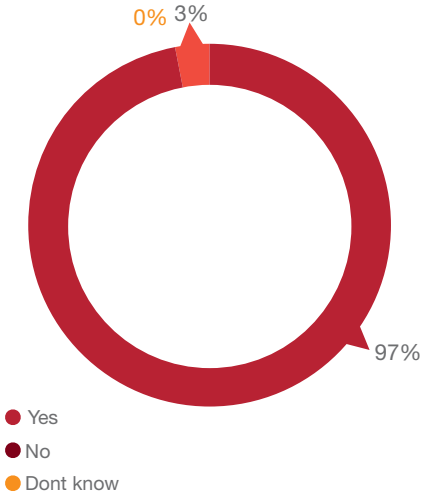
Amount lost as a result of Asset misappropriation in Tanzania



45%

of respondents that suffered economic crime lost TZS 230M or more

Was the most disruptive incident brought to the attention of the Board or senior leaders charged with governance in the organisation?



Who is committing the fraud?

Internal Fraudster

Similar to the trend evidenced globally, most economic crimes continue to be committed by internal actors. Of the incidents of economic crimes suffered by the survey respondents in Tanzania, 68% were perpetrated by internal fraudsters while external actors accounted for 21%. 11% of respondents either did not know who perpetrated the economic crime or preferred not to say. In Africa and globally, the proportion of economic crime incidents perpetrated by internal fraudsters was 56% and 52% respectively.

The results of the survey indicate that junior management was responsible for 50% of the economic crimes committed by staff within organisations in Tanzania. In terms of function, 39% of perpetrators are reported to operate in the Marketing and Sales function, Operations and Production was second at 17%.

Operations and Production was however cited as the function contributing the highest number of fraudsters in East Africa, Africa and Globally. It would be paramount therefore that organisations tighten controls around the Sales and Marketing as well as the Operations and Production functions to combat fraud perpetrated by insiders.

The survey results for Tanzania differ from the Global trend where middle management are responsible for 37% of economic crime committed by staff and junior management account for only 26% of the cases of economic crime reported on a global scale.

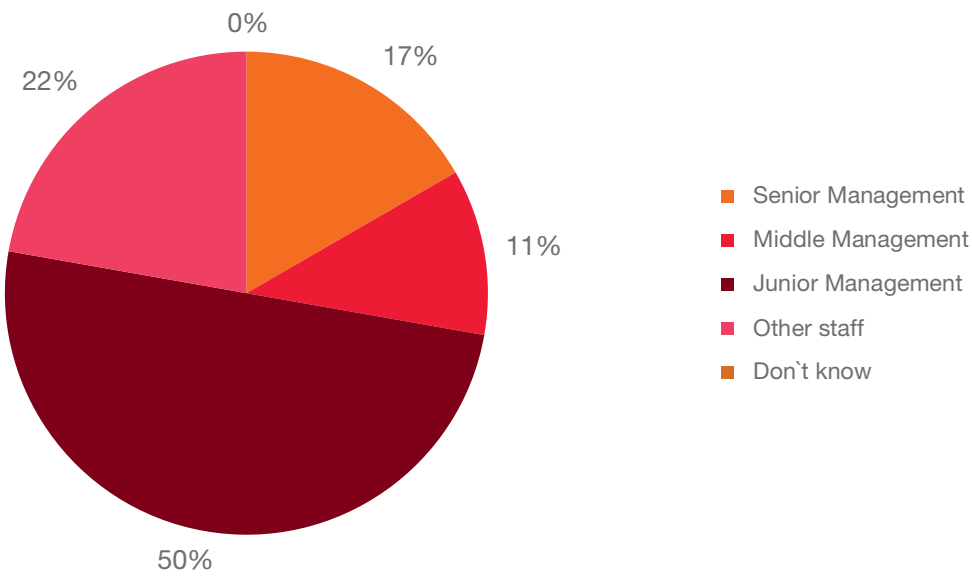
The results shown below could be due to junior management executing majority of the operational and management tasks and by virtue of them having a deeper insight into the weaknesses of the organisation's systems. It therefore behoves the senior management to continuously monitor the actions of their junior teams and employ sufficient supervisory structures and operational controls to curb fraudulent activities by the lower management team.

This does not however mean that senior management are beyond reproach on the matter. Unlike in Tanzania, our survey reveals that the share of serious internal fraud committed by senior management globally continues to rise dramatically — up from 16% in 2016 to 24% in 2018.

68%

of the perpetrators of economic crime were insiders. How thoroughly are you screening your new hires?

Level of Internal Fraudster



1 in 2 economic crimes perpetrated by an internal fraudster is perpetrated by an employee at junior management level

21%

of economic crimes were committed by external perpetrators

External Fraudster

Among the external fraudsters, customers, vendors and agents/intermediaries were all cited as being responsible for most of the economic crimes committed by external fraudsters in Tanzania. Globally and in East Africa, customers were cited as being responsible for the highest proportion of fraud by external parties at 39% and 51% respectively. Hackers and Organised Criminals were rated as second and third.

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

Types of economic crimes

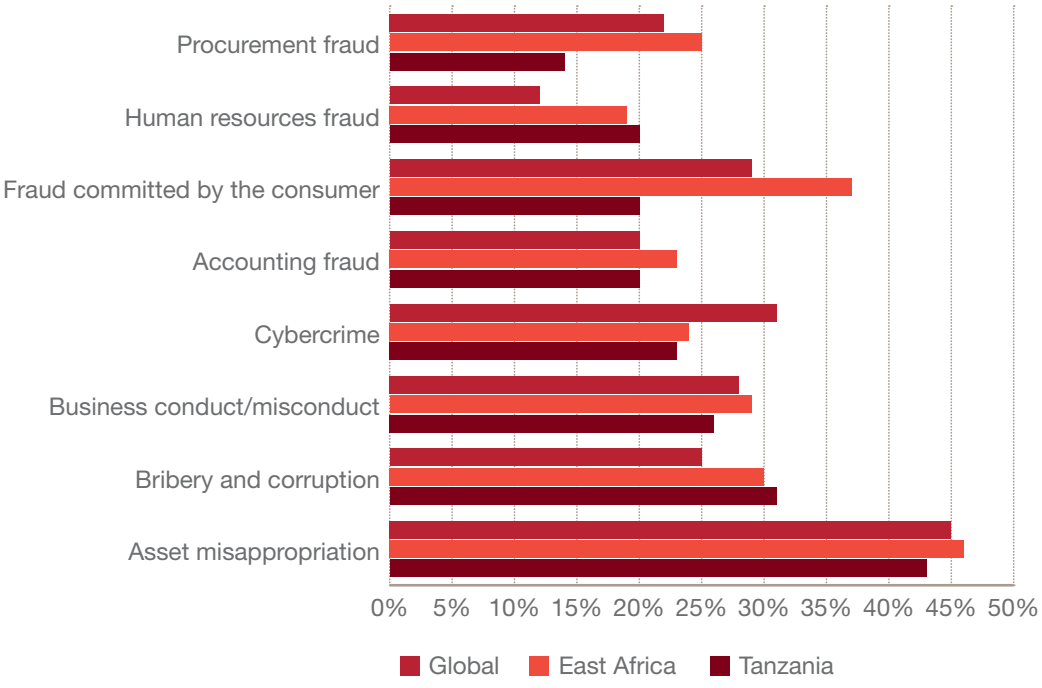
As already noted, Asset Misappropriation continues to be the highest form of fraud experienced by survey respondents globally. The trends on the other economic crimes reported by the survey respondents are as set out in the chart below, where incidents of Bribery and Corruption and Business conduct/ misconduct rank highly in Tanzania as the other common economic crimes encountered.

In this section, we briefly discuss some of the forms of economic crime that we found to be widely experienced in Tanzania.

Top 3

Asset Misappropriation, Bribery and Corruption and Business Misconduct are the most prevalent forms of economic crime in Tanzania

Types of Economic Crime



43%

Prevalence rate of Asset Misappropriation in Tanzania

Asset Misappropriation

As per the survey results, Asset Misappropriation remains the most prevalent economic crime globally. It generally involves the theft or embezzlement of company assets by directors, employees or other fiduciaries.

Asset Misappropriation like other forms of economic crime, 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, without knowledge or consent, the organisation's assets to themselves or to the ownership of a third party.

This crime covers a wide range of nefarious acts ranging from embezzlement of physical assets such as inventory and cash to embezzlement of non-cash proprietary information and intellectual property such as patents and copyrights. It also involves the abuse of organisation assets e.g. improper or irregular use of company vehicles and assets at the expense of the organisation.

Indeed, in stark contrast to the 23% of Tanzania respondents that indicated that Asset Misappropriation was the most disruptive form of economic crime suffered by their organisations in the past 24 months, only 13% of the respondents indicated that they perceived Asset Misappropriation to be the form of crime likely to be most disruptive to their organisations in the next 24 months overtaken by Business Misconduct and Bribery and Corruption which have speculated incident rates of 18% and 17% respectively.

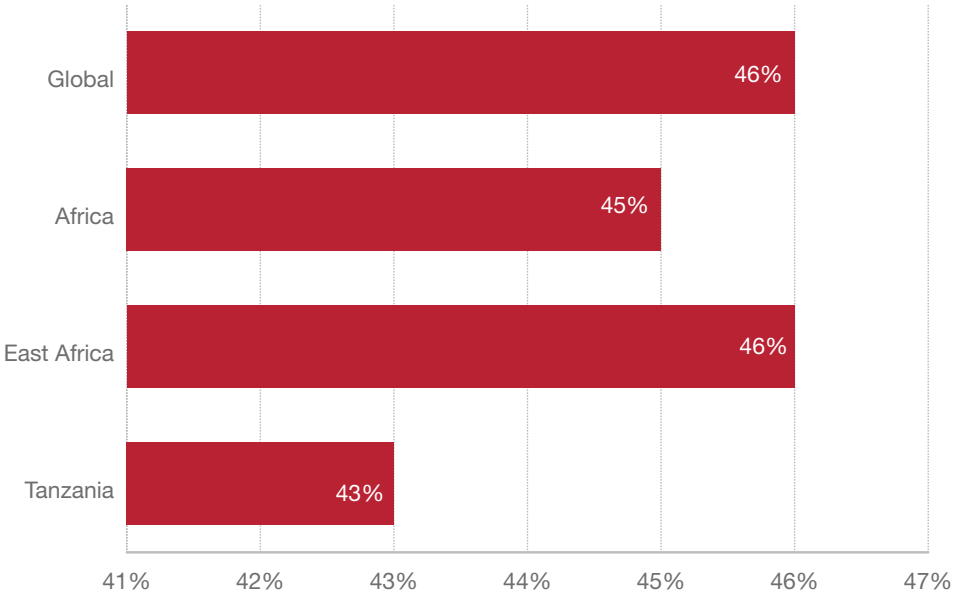
This perception is also held globally, where only 11% thought that Asset Misappropriation is going to be the most disruptive form of economic crime in the next 24 months trailing Cybercrime at 26% and Bribery and Corruption at 12%.

The greatest impact of this form of crime as per the responses from the survey appears to be felt on the organisations' brand and reputational strength as well as on the way organisations relate with each other within Tanzania.

23%

of respondents stated that Asset Misappropriation was the most disruptive form of economic crime they had experienced over the last 24 months

Asset Misappropriation 2018



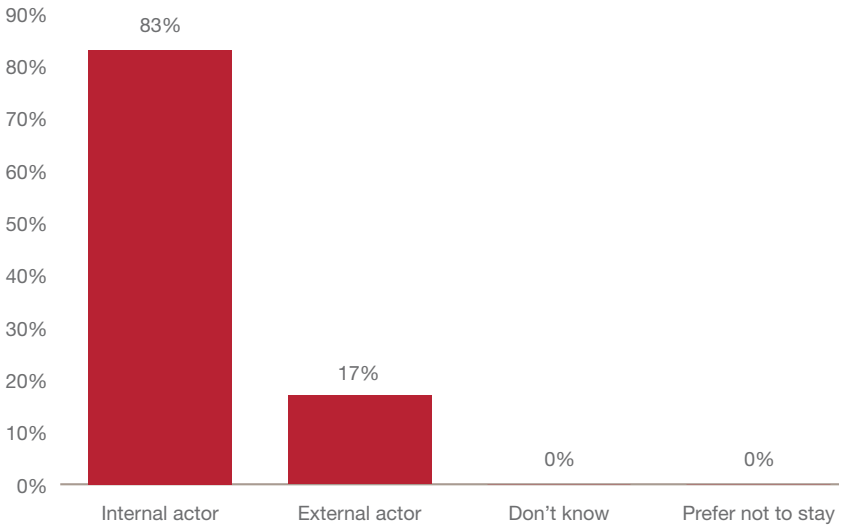
In a highly technologically advanced society, Asset Misappropriation is still widely considered to be a traditional "brick and mortar" form of crime and therefore often overshadowed by other economic crimes that often involve highly sophisticated technological tools.

This lack of interest may have contributed to the incorrect perception that Asset Misappropriation is not as big a threat going forward as other emerging forms of economic crimes for example Cybercrime and Fraud committed by Consumer.

The survey further indicates that 83% of the perpetrators of Asset Misappropriation in Tanzania were employees within the organisation. To curb this vice therefore, it's 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.

Perpetrators of Asset Misappropriation



Africa

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

The organisation culture also plays a big role in influencing the behaviour of staff at all levels. Setting the right tone at the top may sound a cliché, but it plays a big part in shaping the organisation's attitude towards economic crimes from how it is set up to mitigate it to how it deals with it.

Bribery and Corruption – 'sharing' isn't always caring

At 31% incidence rate, Bribery and Corruption is the second most prevalent form of economic crime in Tanzania according to the results of the survey. This is against the 30% incident rate in East Africa, 32% in all of Africa and 25% globally. The proportion of respondents that experienced incidents of Bribery and Corruption is observed to be consistently larger in African countries than in the rest of the world, showing how endemic the vice is and putting into the spotlight the vigilance and enforcement of regulations in place to curb the vice.

26%

Prevalence rate of Business Misconduct in Tanzania

Tanzania has in place a robust legal framework designed to counter occurrences of Bribery and Corruption. However, just as in most countries in Africa, enforcement requires to be tightened. The enactment in 2007 of the Prevention and Combating of Corruption Act (PCCA) and the consequent establishment of the Prevention and Combating Corruption Bureau (PCCB), were major milestones in the fight against corruption. The PCCA was aimed at implementing the UN Convention against Corruption (UNCAC) and the African Union Anti-Corruption Convention. It added new legal provisions such as the criminalisation of gift giving and of the use of facilitation payments.

With this robust set of regulations in place, it is incumbent upon the agencies charged with the investigation and prosecution of acts of corruption to be more engaged and vigilant in their enforcement of the law to ensure that Bribery and Corruption decreases. Our leaders and especially religious leaders, teachers and parents also have a role to play in bringing up a generation that perceives Bribery and Corruption as unacceptable and intolerable.

Business conduct/misconduct

According to the survey results, Business Misconduct stands as the third most prevalent economic crime experienced by Tanzanian organisations recording a prevalence rate of 26%. Business Misconduct generally 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.

Globally, corporates spend a significant share of their revenues every year in dealing with lawsuits filed against them following cases of unethical conduct including copyright infringements, anti-competitive behavior, child labour and environmental pollution. Some employers have been sued for threatening or firing whistle-blowers, or employees who point out illegal practices or safety violations in the workplace. Some businesses go as far as using undocumented workers because they can pay them less. In the procurement function some businesses engage in bid rigging, an unethical practice where a commercial contract is promised to one party even though for the sake of appearance several other parties also present a bid.

In the financial scheme of things, businesses may engage in financial misconduct by undertaking activities such as paying unjustifiable salaries and bonuses to top officials regardless of work performance, sometimes in spite of it and chasing short-term profit by placing investor's money in questionable investments. Corporate misrepresentation may also take the form of product misrepresentation where an organisation fraudulently claims that their products offer certain benefits.

Dealing with cases of business misconduct requires the adoption of zero tolerance attitudes towards unethical behavior and the cultivation of a culture of ethical business practices that transcends all levels of the organisation particularly spearheaded by executive management who set the tone at the top.

Organisations can regulate business conduct by having a robust Code of Ethics or Code of Business Conduct in place and ensuring stringent compliance with the same. In its part, government can assist to mitigate this by strengthening regulation and empowering the agencies charged with regulation of areas where such misconduct may manifest to deal with such cases and deter their occurrence.

Focus on Cybercrime and Fraud Committed by the Consumer

Cybercrime - A disconnect between means and ends

Cybercrime, also known as a computer crime, is an economic crime committed using digital devices such as 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 these devices and it is very relevant in the East African context where growth in the use of mobile phones has provided computing ability and internet access to a large proportion of the 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 rise of technology has exposed organisations to a number of threats, the key ones being:

- **Hacktivists —** this is an individual who gains unauthorized access to the computer files or networks of organisations in a bid to convey a social or political message. Threats include service disruptions or reputational damage; victims often include high-profile organisations and governments
- **Insiders —** not only employees but also trusted third parties with access to sensitive data
- **Organised crime syndicates —** threats include theft of financial or personally identifiable information (sometimes with the collusion of insiders); victims often include financial institutions, retailers, medical and hospitality companies.

In Tanzania, Cybercrime is the fourth most prevalent form of economic crime at an incident rate of 23%. The incidence rate within the Financial Services sector in Tanzania was even higher with 45% of the respondents within this category that had suffered economic crime citing it as one of the forms of crime they had suffered.

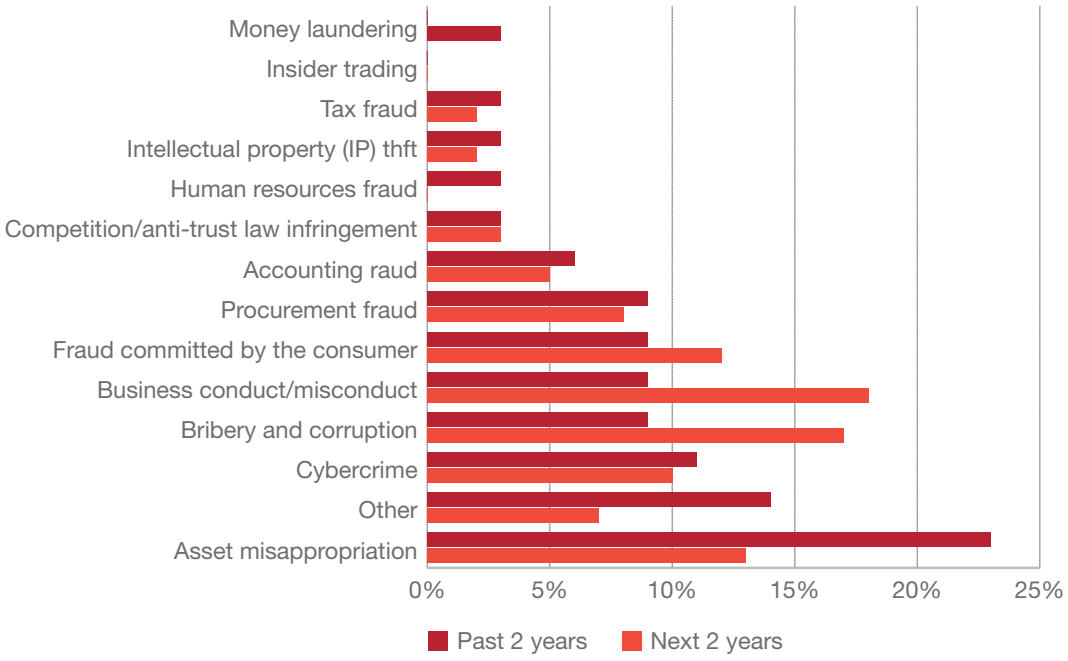
This was second only to Fraud Committed by the Consumer that had an incidence rate of 55%. However, 33% of the respondents feel that Cybercrime has the potential to be the most disruptive crime within the Financial Services sector in the next two years, trouncing Fraud Committed by the Consumer at 25%.

Across all sectors and in terms of level of disruption, 11% of the respondents in Tanzania reported Cybercrime as the third most disruptive economic crime.

45%

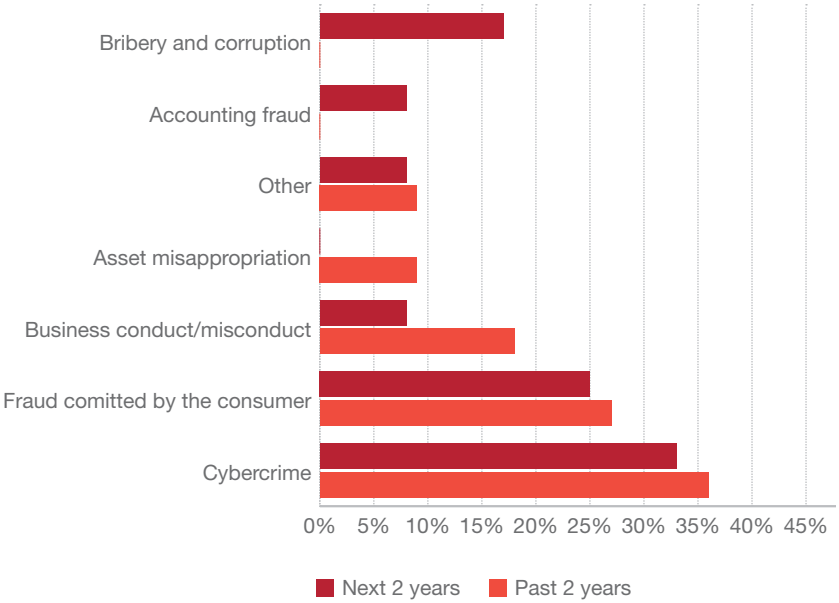
the prevalence rate of cybercrime in the financial services sector, which is double the overall Tanzania cybercrime prevalence rate

Comparison between experience and perception of the disruption caused by various forms of economic crime



In general, respondents rate Business Misconduct and Bribery and Corruption as the crimes of the future

Comparison between experience and perception of the disruption caused by various forms of economic crime in the Financial Services Sector within Tanzania



The financial services sector rates cybercrime as likely to be as the most disruptive form of economic crime going forward

1 in 2

respondents who suffered cybercrime did not understand the specific technique of cyber-attack employed

The rapid advancement of technological tools and solutions brings in its wake additional opportunities for cyber criminals to perpetrate crime. The digitization of system processes and transactions also means that these fraud opportunities are increasing exponentially making Cybercrime a growing threat to businesses and organisations throughout the globe.

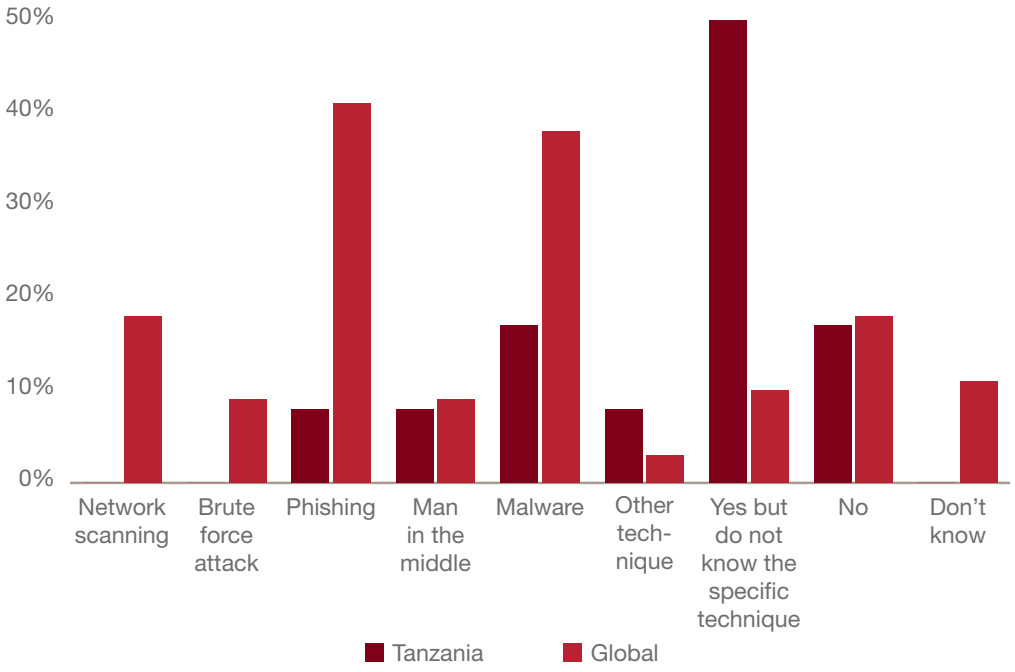
Additionally, the high demand for digital solutions and alternatives e.g. online banking, online payment solutions and digital currencies coupled with the relatively low understanding of these new technologies by organisational leadership, is leading to new markets and added incentives for hackers and fraudsters. In fact, cyberattacks have become so pervasive that measuring its occurrences and impact is becoming less strategically useful than focusing on the mechanism that the fraudster used.

Of the respondents in the Financial Services sector in Tanzania who cited having suffered from Cybercrime in the last 24 months, it appears that 50% of the respondents were not aware of the specific Cybercrime technique used.

This paints a very grim picture showing the possible reluctance of these organisations to arm themselves with the requisite knowledge and techniques necessary to ward off incidences of Cybercrime especially with the high prevalence rates of the crime in the sector.

This can lead to a situation where the organisations administer a 'universal panacea' and fail to take precautions that are tailored to the threats of Cybercrime they are most exposed to, which is essentially no different from taking no precautionary action at all. It may as well end up being a case of administering the wrong medicine for an unknown illness. This information is demonstrated in the graph below:

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



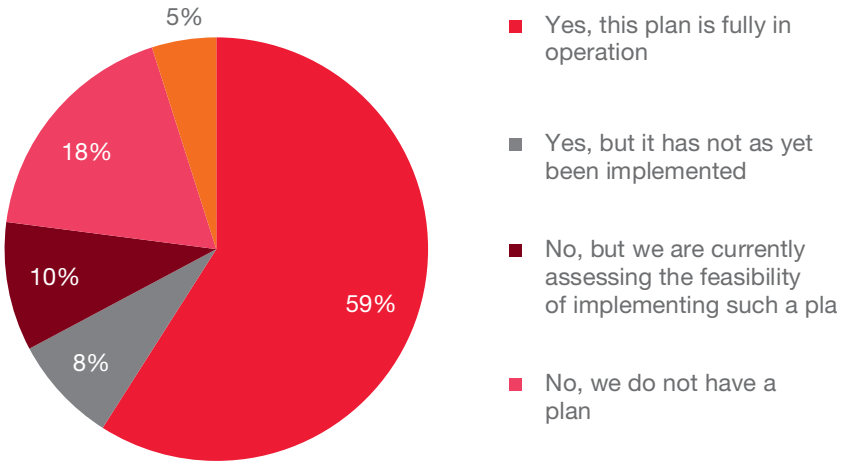
Phishing and Malware are likely to be the most prevalent techniques of cybercrime employed

59% respondents from organisations in Tanzania reported that they have a fully operational Cyber Security Program in place while 18% reported not having one in place. Considering the fact that Cybercrime is viewed as the fourth most prevalent economic crime in the country, an improvement in these numbers is necessary as this is a crime that is rapidly and constantly evolving.

The borderless nature of Cybercrime also complicates the ability of most institutions to deal with the threat, and the laws developed to deal with the threat are not legislated at the same pace as the level of sophistication cybercriminals upgrade their attacks.

This is one of those economic crimes that would require a concerted global effort to be adequately dealt with given its borderless nature.

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



Fraud committed by the Consumer – focus on customer

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

For the first time, the 2018 Survey included Fraud Committed by the Consumer as a new economic crime classification. This classification relates to a 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 indicate that this crime had a prevalence of 37% within the East African region making it the second biggest threat to organisations after Asset Misappropriation. In the Financial Services sector in Tanzania, Fraud Committed by Consumer recorded a 55% incidence rate, becoming the most prevalent form of economic crime within the Financial Services industry in Tanzania.

This crime is also the most prevalent globally in the Financial Services sector trailed closely by Cybercrime. The vice was especially prevalent in the Banking and Capital markets sub-sector where it had an incidence rate of 60% becoming the most prevalent form of economic crime, ahead of Cybercrime and Asset Misappropriation which have traditionally been the leading forms of economic crime in that industry.

Your customers are the lifeblood of your business. As businesses continue to trudge through the digital and global revolution, they are today forced to innovate, enter new markets and adopt new technologies in order to survive or grow. This opening up however also exposes the businesses to additional threats, often posed to, and by the customer.

4th

Fraud Committed by the Consumer was the fourth most prevalent form of economic crime in Tanzania at 20% prevalence rate

This rings true also for organisations such as governments and non-profit organisations where the consumer of their services is not necessarily a customer. Organisations are therefore faced with a dilemma of either closing themselves in and be seen as non-responsive or opening up their operations and exposing themselves to financial, reputational and regulatory risks. In this section we discuss the consumer and the fraud risk that they portend.

Why is the threat from the customer on the increase

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.

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, tellers have given way to mobile banking and parking attendants to parking 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.

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.

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, manufacturers get into real estate and the government begins to sell bonds through mobile apps, they all find themselves in unfamiliar territory that is fraught with danger.

Finally, in societies where the cost of living is increasing, lifestyle trends promote more consumerism and traditional values are discarded, the consumer just as 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 is a case of shoplifting.

Technological advances have given customers more access to organisations' systems, availing more opportunities for fraud

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 go a long way in helping single out suspicious persons or imposters or abnormal transactions.

KYC

Are your customers who they say they are?

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

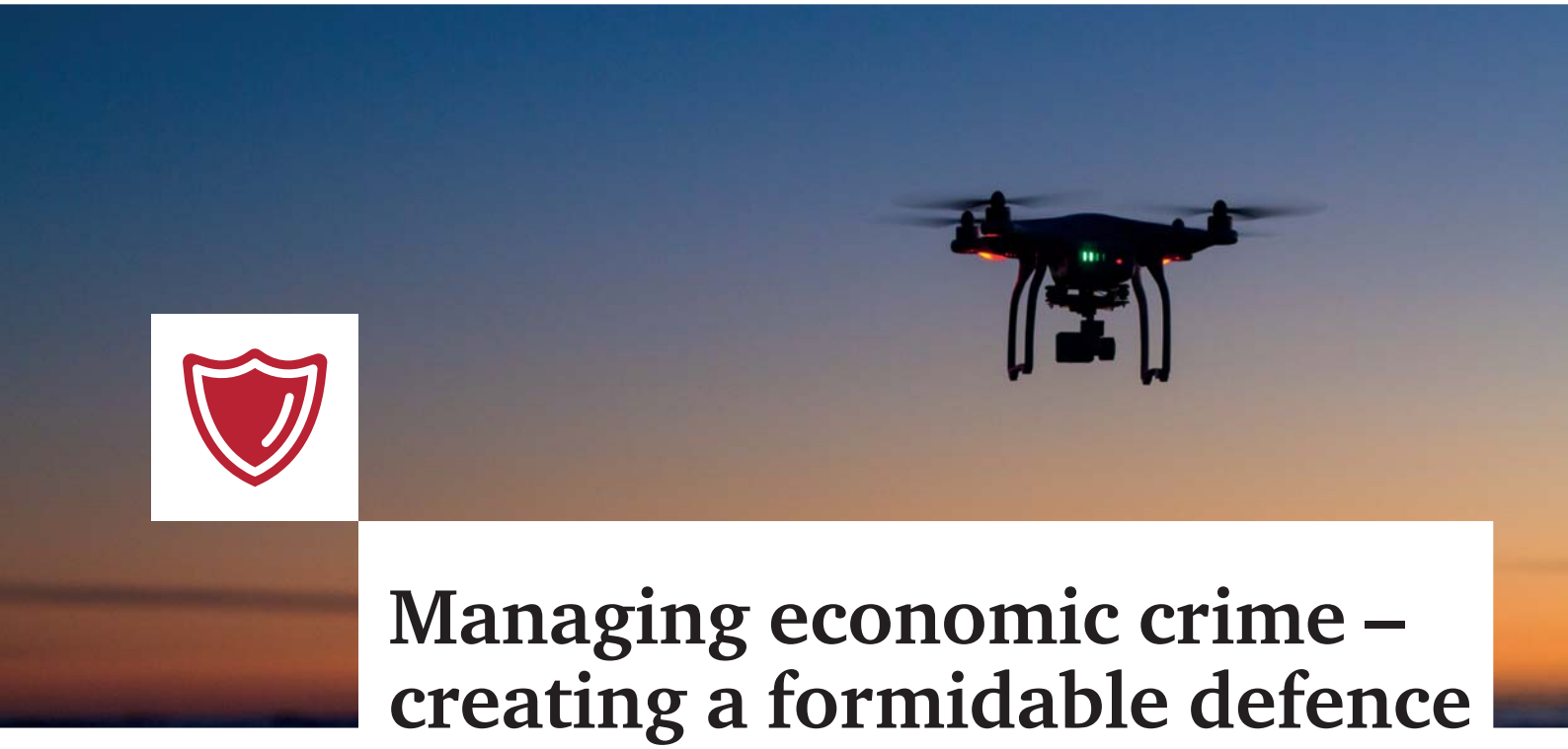
Risk Management Procedures

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 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 Money Laundering activities

With regard to legislative measures to curb fraud perpetrated by the consumer, the Bank of Tanzania has continued to exercise its statutory role in the Financial Services sector to ensure that payment systems are modernised, efficient and most importantly secure. This has been done through instituting a framework that covers a number of laws including the Electronic Transactions Act (2015) and Cybercrimes Act (2015). Under these frameworks, a provider of payment systems must first obtain a license from the regulator before operating any system. This is commendable and should be sustained.



Managing economic crime – creating a formidable defence

54%

of Tanzanian respondents cited corporate controls as the means by which their most disruptive economic crime was detected

Don't get blindsided by your blind spots

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, 84% of our respondents reported having insight into fraud and/or economic crime incidence in their organisation on a global level. In Tanzania, this statistic is notably higher than the global average where 93% of our respondents in Tanzania reported having insight into fraud and/or economic crime incidence in their organisation.

Given that success in the prevention, detection and management of economic crime in its entirety primarily depends on the ability of key parties in that organisation to recognize the nature and type of economic crime the organisation frequently faces or is likely to face, these results are encouraging.

However, a small percentage (7%) of the respondents reported having either limited or no insight at all into the prevalence of economic crimes in their organisation. In such cases 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.

Detection of economic crimes – your arsenal

The survey reveals that in order to detect and manage fraud dynamically, all the facets of fraud detection mechanisms 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 is encouraged and upheld by all stakeholders.

Against a global average of 51%, 54% of our Tanzania respondents cited corporate controls as the means by which their most disruptive economic crime was detected. Suspicious activity monitoring, fraud risk management exercises and routine internal audits were cited as the top three corporate control tools employed by the respondents by which the organisations' management were able to detect the perpetration of economic crimes.

Another emerging corporate control cited by the respondents as the means through which economic crimes at their organisations were detected was data analytics.

It is encouraging to note that in this survey, a good number of the responses from Tanzania reported having carried out fraud risk assessment with the focus being on general fraud risk assessments, cybersecurity and anti-Bribery and Corruption

13%

of respondents had not performed any risk assessments in the last 24 months, a low but still concerning percentage

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

reviews. 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 be indicative of irregular or fraudulent activities.

Invest in people, not just machines

25% of our Tanzania 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 well 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.

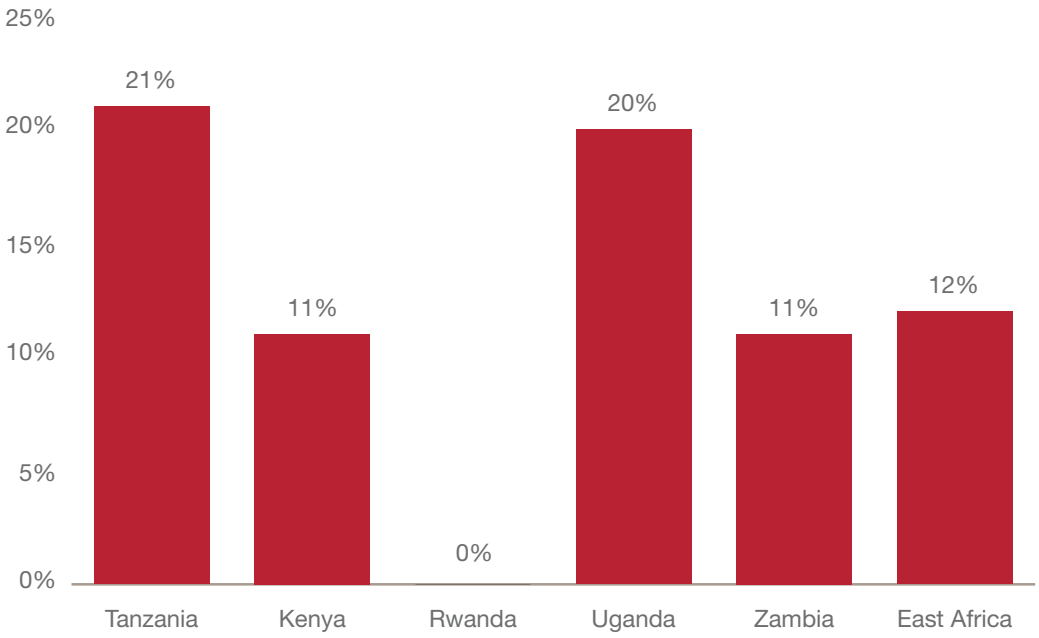
Beyond the influences of management

21% of our respondents indicated that their most disruptive economic crimes were detected beyond the influences of management, either by accident, by an unspecified method or through an unknown method. This is very high compared to other countries in the East African region, where the regional average is 12%. Neighbouring Rwanda has an incidence rate of 0% for economic crimes that are beyond the influences of management, this disparity is glaringly large. 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.

This may also be an indicator that the controls in place to mitigate economic crime may not be sufficient, and the incidents only come to light when perpetrators or their conspirators volunteer the information. The graph below demonstrates the responses gathered from the countries within East Africa.

Beyond the influence of Management



Fraud detection that is beyond management's influence suggests that there may exist significant risks that have yet to be identified and/or mitigated

As organisations use technology to improve efficiencies, they should also think about how it may be employed to prevent/detect fraud

Prevention of economic crimes

Find the right technology to fight fraud – finding the sweet spot

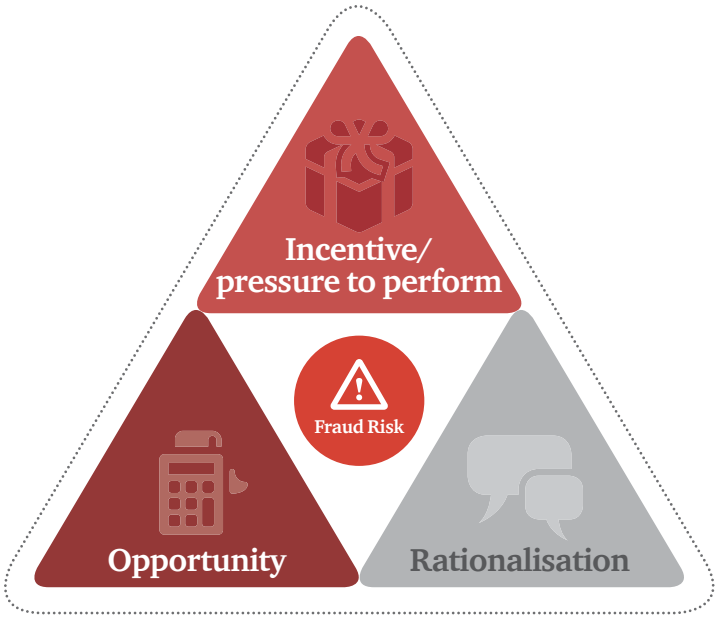
With new emerging technologies many of which can be exploited to perpetrate crime, organisations need to be vigilant and conduct an in-depth assessment of the right technology to serve the requirements of the organisation taking into account factors such as the size of the organisation, type and volume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

The continuous, periodic and proactive monitoring and analysis of organisation's systems including transactions, 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; 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.

The antidote to pressure - Openness

Corporate-targeted frauds are often connected to corporate pressures including unreasonable targets, job insecurity, which 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 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 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.

Controls are as good as the individuals enforcing them, so organisations should ensure that while they invest in the best systems and processes to tighten the controls, they also have individuals with the right skill sets to enforce the controls. Tanzanian respondents perceive opportunity as the greatest contributor to the execution of a fraudulent activity with 63% 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 is where the perpetrator of the fraud reconciles 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. Using surveys, focus groups and in-depth interviews, to assess the organisation's culture's strengths and weaknesses, and focus on the 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. The organisation's culture is also set by the leadership, as junior staff often mirror what their leaders do in the organisation, or adapt their code of ethics to what they observe as the overarching set of behaviours being displayed by the leadership.

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

An East African view of Economic Crime

Prevalence of economic crimes

For the first time since the launch of GECS in 2001, we compare the Tanzania results against those of other East African countries and in particular: Kenya, Uganda, Rwanda and Zambia. Whereas we have had country specific reports and statistics in Kenya since 2010 and in Zambia since 2014, it is the first time that we had enough responses to generate reports from Tanzania, Uganda and Rwanda.

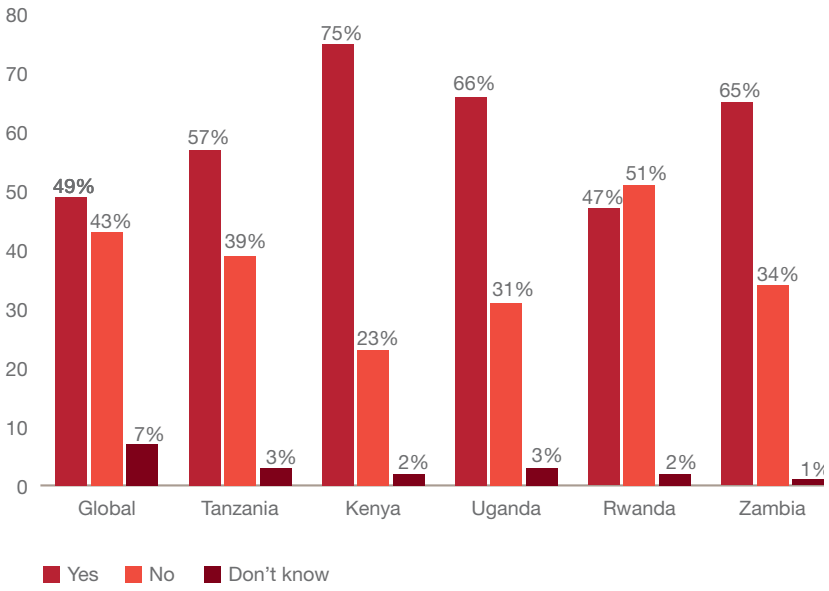
Against the global rate of 49%, the East African region reported a 62% average prevalence of economic crime in the last 24 months, with Kenya having the highest prevalence rate at 75% and Rwanda the lowest at 47%, just below the global average of 49%. It is also worthwhile noting that from the results of the survey, Tanzania is surpassed only by Rwanda making it the second country within the East African region with the lowest incidents of economic crime at an incidence rate of 57%.

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 be cross-border cooperation in formulating and implementing policies that help prevent, detect and mitigate against various forms of economic crimes.

62%

the reported prevalence rate of economic crime in East Africa

Has your organisation experienced any fraud and/or economic crime in your country within the last 24 months?

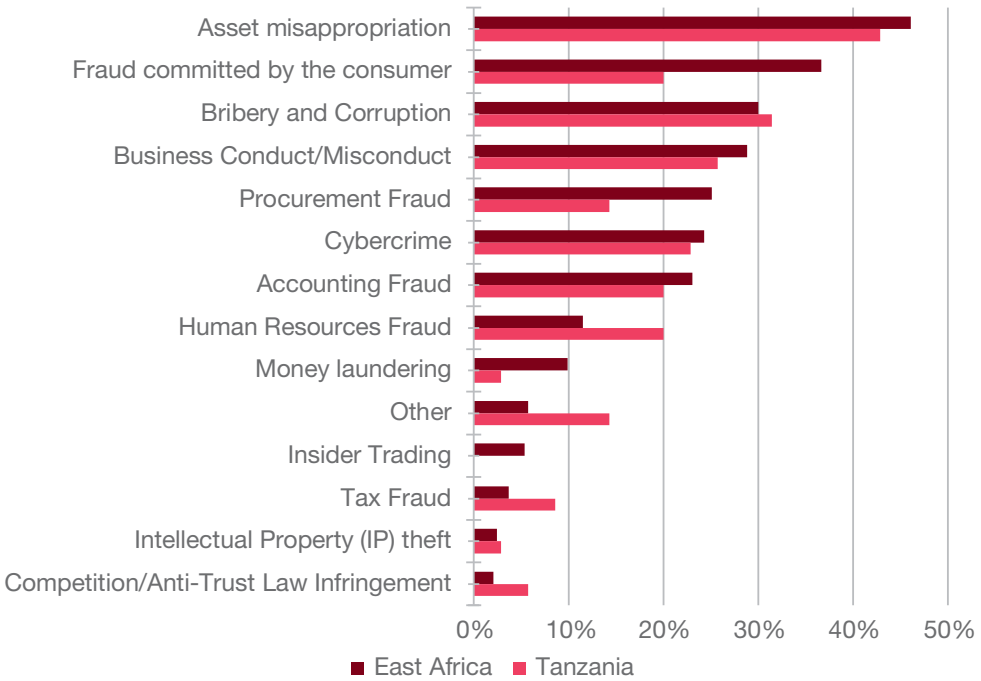


Types of economic crimes experienced in East Africa

On average, the top three forms of economic crimes most experienced in East Africa were Asset Misappropriation (46%), Fraud Committed by the Consumer (37%) and Bribery and Corruption (30%).

Different forms of economic crimes are experienced differently in the East African region. Whereas Fraud Committed by the consumer is the second most prevalent economic crime in Kenya and Rwanda at incident rates of 37% and 39% respectively, it is the most prevalent economic crime in Uganda at a prevalence of 45%. In Tanzania, the threat posed by Fraud Committed by the Consumer is relatively low at

Types of Economic crime experienced in East Africa



an incidence rate of 20%. In the Financial Services sector within Tanzania, the prevalence of Fraud Committed by Consumer is however higher with a prevalence rate of 55%.

Zambia takes the lead as the regional country with the highest prevalence rate for two of the three major economic crimes experienced in East Africa. With the exception of Uganda, Asset Misappropriation has the highest incidence rate in all the East African countries.

From the responses received it is apparent that the trends in economic crime are relatively similar in most East African countries with the top three economic crimes experienced being Asset Misappropriation, Fraud Committed by Consumer and Bribery and Corruption. In Tanzania however, the trend is a bit different where most respondents feel that incidents of Business Misconduct are relatively high at an incidence rate of 26%. This is shown in the chart below.

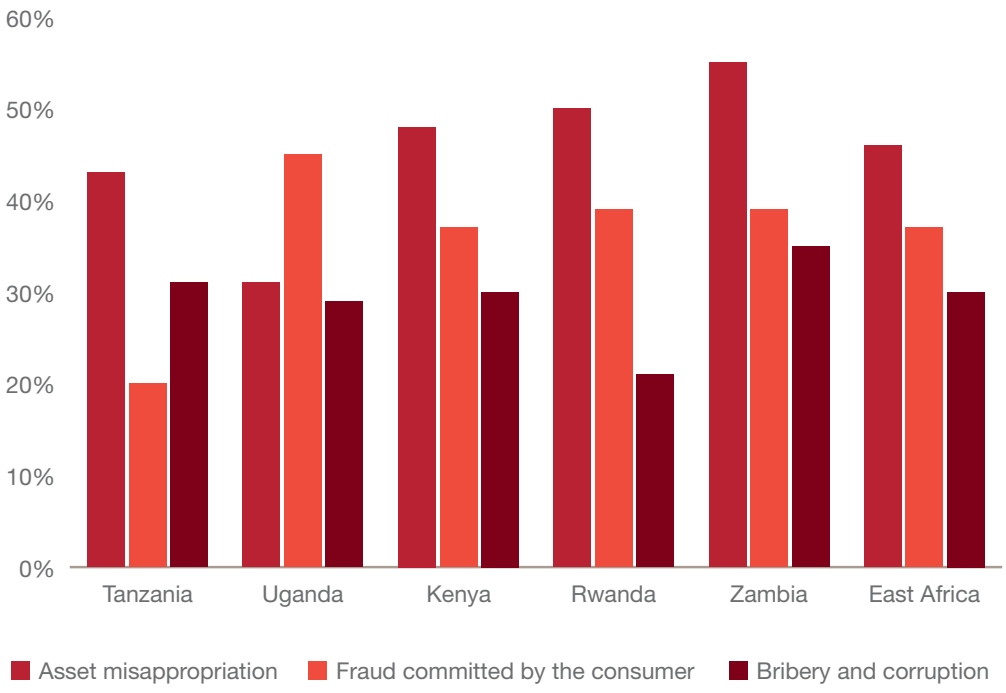
The financial losses resulting from the most disruptive economic crimes in Tanzania are also vaguely similar to the results from the East African region at large.

In Tanzania, 31% of the respondents reported to have lost between USD 100K and USD 1M to the most disruptive forms of economic crime experienced in the past 24 months of operation. This is against 24% of East Africa respondents that reported to have lost the same amount. In both instances this was the highest range reported as being lost to the most disruptive forms of economic crime.

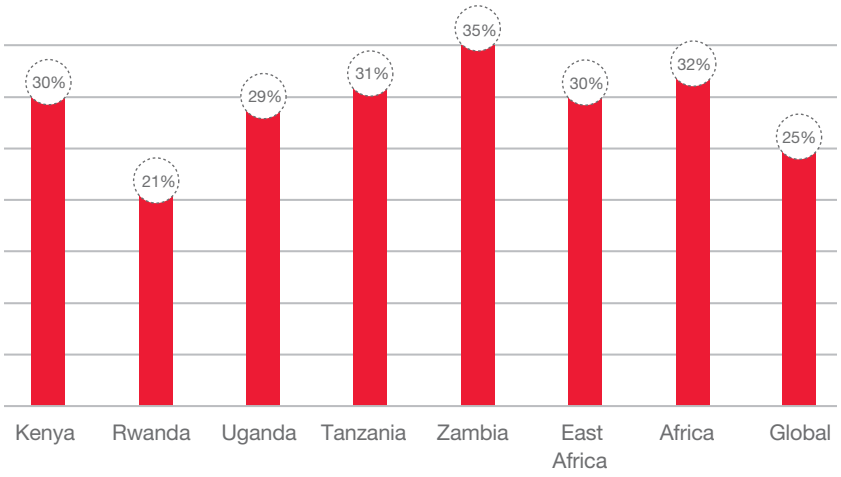
Of the responses received from East Africa, 30% reported that they experienced Bribery and Corruption in their organisations within the last 24 months, making it the fourth most prevalent form of economic crime in East Africa. At 35%, Zambia has the highest prevalence of Bribery and Corruption trailed closely by Tanzania where Bribery and Corruption has a prevalence rate of 31% rendering it the second most prevalent crime in Tanzania surpassed only by Asset Misappropriation. The least incidence rate of Bribery and Corruption observed in Rwanda stands at 21% making it the only country

Other than Fraud Committed by the Consumer, (which is noticably less prevalent) the prevalence of the other forms of economic crime in Tanzania ressemble those in the East Africa region

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



Prevalence of Bribery and Corruption



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

within East Africa with incidences of Bribery and Corruption below the global average of 25%.

In Tanzania, 23% of the respondents reported to have been asked to pay a bribe in the last 24 months in their primary country of operations. Similarly 23% 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.

In neighbouring Rwanda, 71% of the respondents reported that they had not been asked to pay a bribe in the last 24 months. This is significantly higher that the averages reported within the East African and Continental levels which stand at about 50%.

Bribery and Corruption is a problem that transcends sectoral and regional boundaries. It is therefore critical that all players of the economy converge and direct their efforts towards creating social and economic accountability mechanisms to curb this vice.

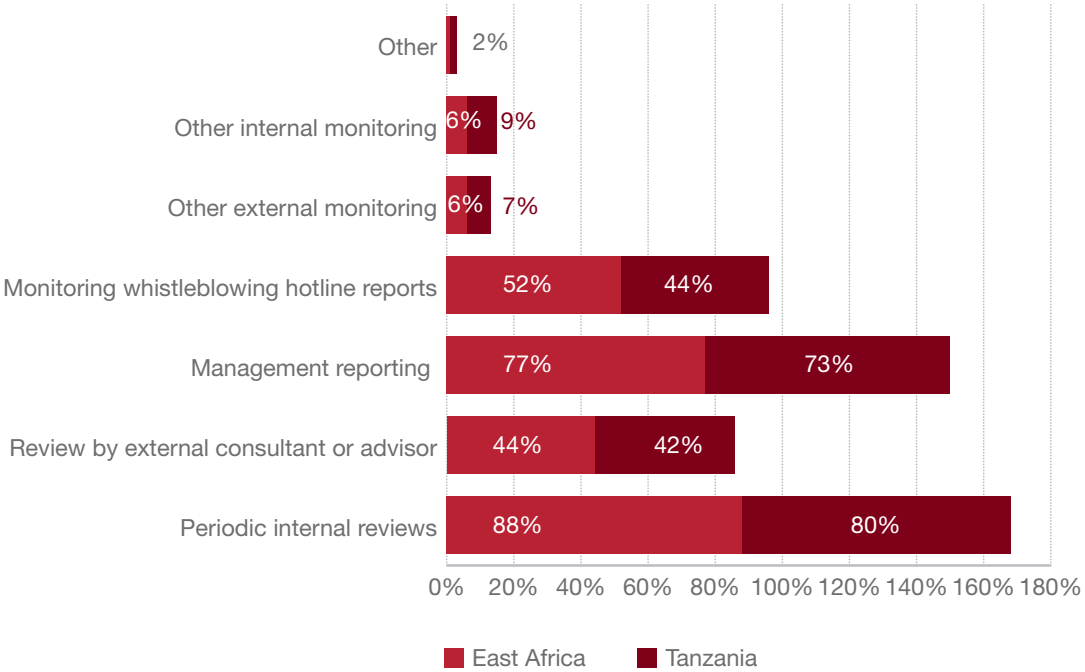
Compliance and business ethics programmes

According to the results of the survey, 80% of Tanzania 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 effectiveness of compliance and business ethics programmes include management reporting and monitoring of whistleblowing reports. Only 42% of Tanzania respondents and 44% of East Africa respondents indicated that they used an external consultant or advisor in the monitoring of compliance issues. This is of concern.

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

Our survey shows that many organisations are still under-prepared to deal with economic crime 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, software, 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 you didn't know you had.

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; 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

David Tarimo
Country Senior Partner, PwC Tanzania
+255 (0) 22 219 2600
david.tarimo@pwc.com

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

Patrick Kiambi
Partner, PwC Tanzania
+255 (0) 22 219 2311
kiambi.patrick@tz.pwc.com

Eric Owino
Forensics Senior Manager
+254 20 285 5692
eric.owino@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 Tanzania, the Survey was completed by 61 respondents making Tanzania one of the 54 countries that achieved the threshold for a country-specific report. Of the 61 respondents, 33% represented listed companies, 56% private organisations while the remaining 11% included government/state-owned enterprises and non-governmental organisations.

www.pwc.com/tz