Economic crime: a threat to business processes

45%
Report having experienced some form of economic crime

81%
Say asset misappropriation is the leading economic crime in Zambia

54%
Of economic crimes were committed by junior staff members

pwc

The PwC Global Economic Crime Survey continues to be the world's leading research programme into economic crime

Contents

This is the first time that Zambia has participated in PwC's Global Economic Crime Survey.

Economic crime in 2014:
The big picture

Welcome to the 7th biennial Global Economic Crime Survey, the largest of its kind ever undertaken both Globally and in Zambia. The survey reveals that economic crimes are a serious threat to business processes and systems and what organisations are doing to mitigate the risks. With over 5,000 respondents, from senior executives in 99 countries, this is the most comprehensive survey of economic crime available to businesses Globally, in Africa and in Zambia. It includes 83 respondents from Zambia, 124 from Kenya, 134 from South Africa and 82 from Nigeria. This survey was conducted between September and October 2013.

This summary report focuses on the results from Zambia based on the Global survey. It seeks to understand and explore trends among economic crimes-including asset misappropriation, bribery and corruption, money laundering and competition law/anti trust law among others and the reasons behind them. It also aims to assess specifically the prevalence and effects of these economic crimes on organisations, and how effectively organisations are dealing with the threats of economic crime.

In this report, the responses from Zambia participants are compared with those from the rest of Africa and Globally, and with the Global results from the 2011 survey. The 83 responses from the 2014 survey came from senior representatives of large, medium and small organisations. Of these, 50% are listed companies, 30% are private companies and 17% are government/public sector organisations. Consequently, the survey provides a useful indicator for evaluating economic crime and trends for Zambia both regionally and Globally as well as the development of fraud trends over the last 2 years.

Asset misappropriation is the leading form of economic crime (both Globally and in Zambia) being 69% at a Global level and 81% in Zambia. Bribery and corruption remains the second most prevalent form of economic crime in Zambia with 35% of respondents reporting incidences against Africa's and Global incidences reported at 39% and 27% respectively. On a regional and Global perspective, procurement fraud was the second highest form of economic crime, coming in at 43% for Africa and 29% Globally, while Zambia had 30% of respondents reporting incidences of procurement fraud.

In this summary report we present the survey findings from Zambia including:

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

In this report, we will focus on asset misappropriation, bribery & corruption, procurement fraud, money laundering, competition law/anti trust law and cybercrime and how organisations can better safeguard themselves against these threats.

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

45% of Zambian respondents reported some form of economic crime while 14% did not know whether their organisations experienced economic crime in the past 2 years.

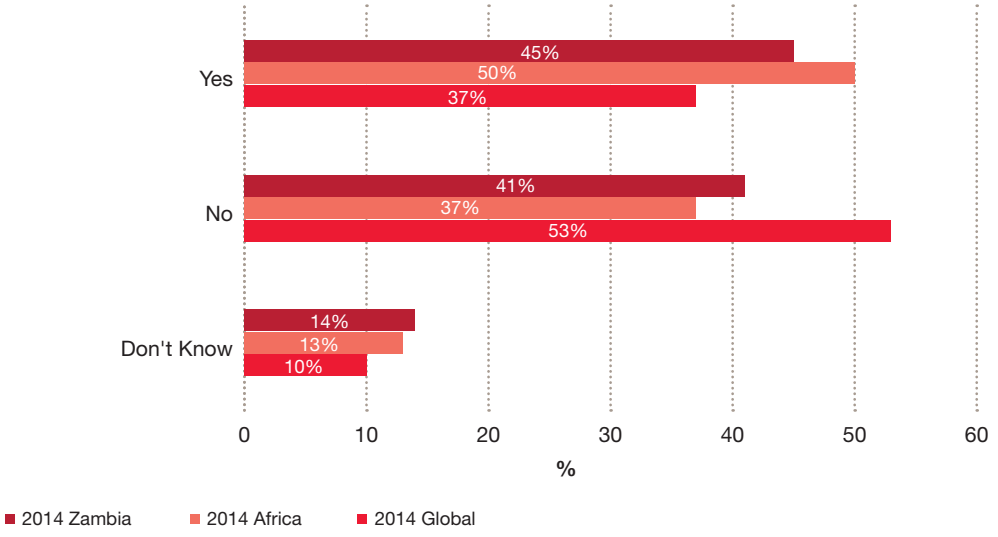
Economic crimes in Zambia

What is happening?

Among Zambian respondents who reported having experienced economic crime over the last 24 months, 45% reported experiencing some form of economic crime compared to 50% in Africa. Globally there was a slight increase of reported incidences of economic crime from 34% in 2011 to 37% in 2014.

Among respondents in Zambia who reported incidences of economic crime, 81% named asset misappropriation as the most prevalent form of economic crime. In Africa, 79% of respondents reported the same while Globally it was 69% of respondents. This is a clear indicator that asset misappropriation Globally is the leading economic crime. This could be due to the fact that asset misappropriation encompasses a wide range of economic crimes and fraud cases.

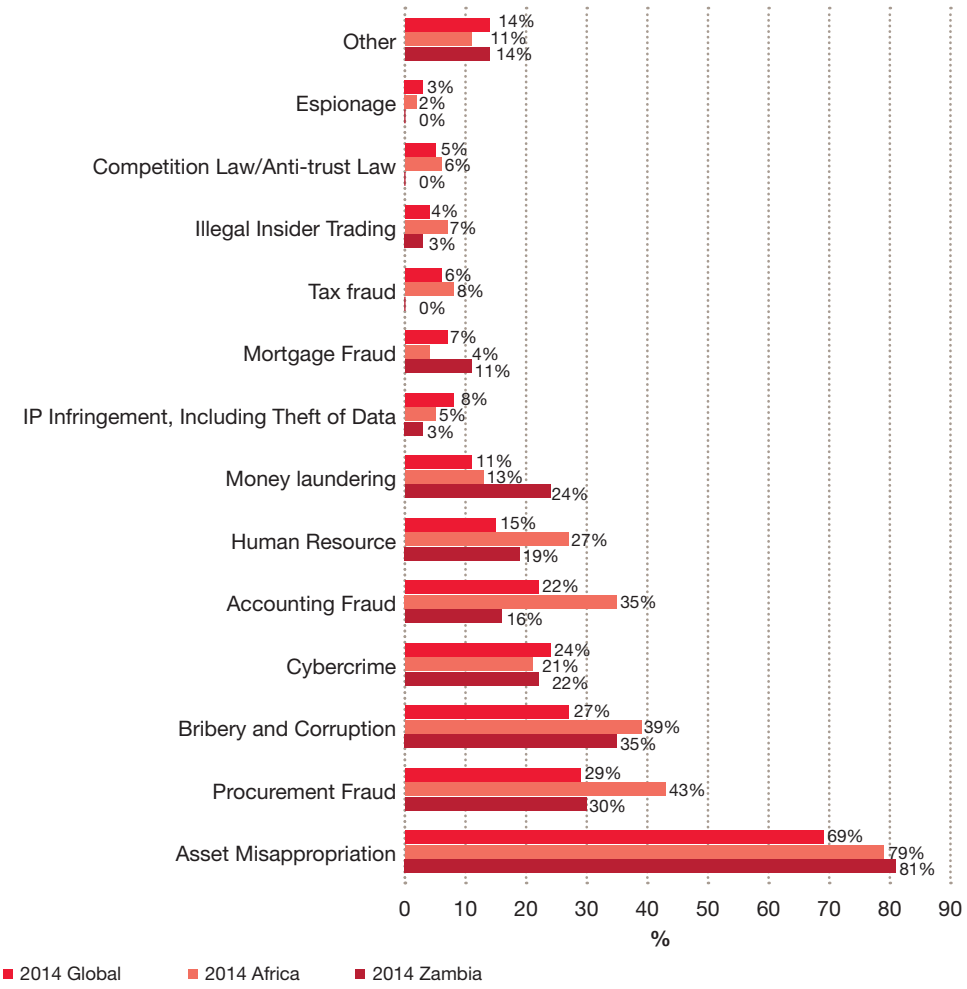
Figure 1: Economic Crime Suffered:



Asset misappropriation (including embezzlement and deception by employees) is defined as theft of organisation resources (including monetary assets/cash or supplies and equipment) by directors, others in fiduciary positions or an employee for their own benefit. Procurement fraud also falls into this category and is a highly ranked crime in Zambia after bribery and corruption. 30% of Zambian respondents reported incidences of procurement fraud compared to 43% of African respondents and 29% of Global respondents. Globally and in Africa, procurement fraud was the second most prevalent form of economic crime recorded.

The second most prevalent form of economic crime suffered by Zambian respondents was bribery and corruption with 35% reporting such incidences compared to 39% in Africa and 27% Globally. On the other hand, procurement fraud ranked the second most prevalent form of economic crime both in Africa and Globally with 43% and 29% respectively.

Figure 2: Types of Fraud



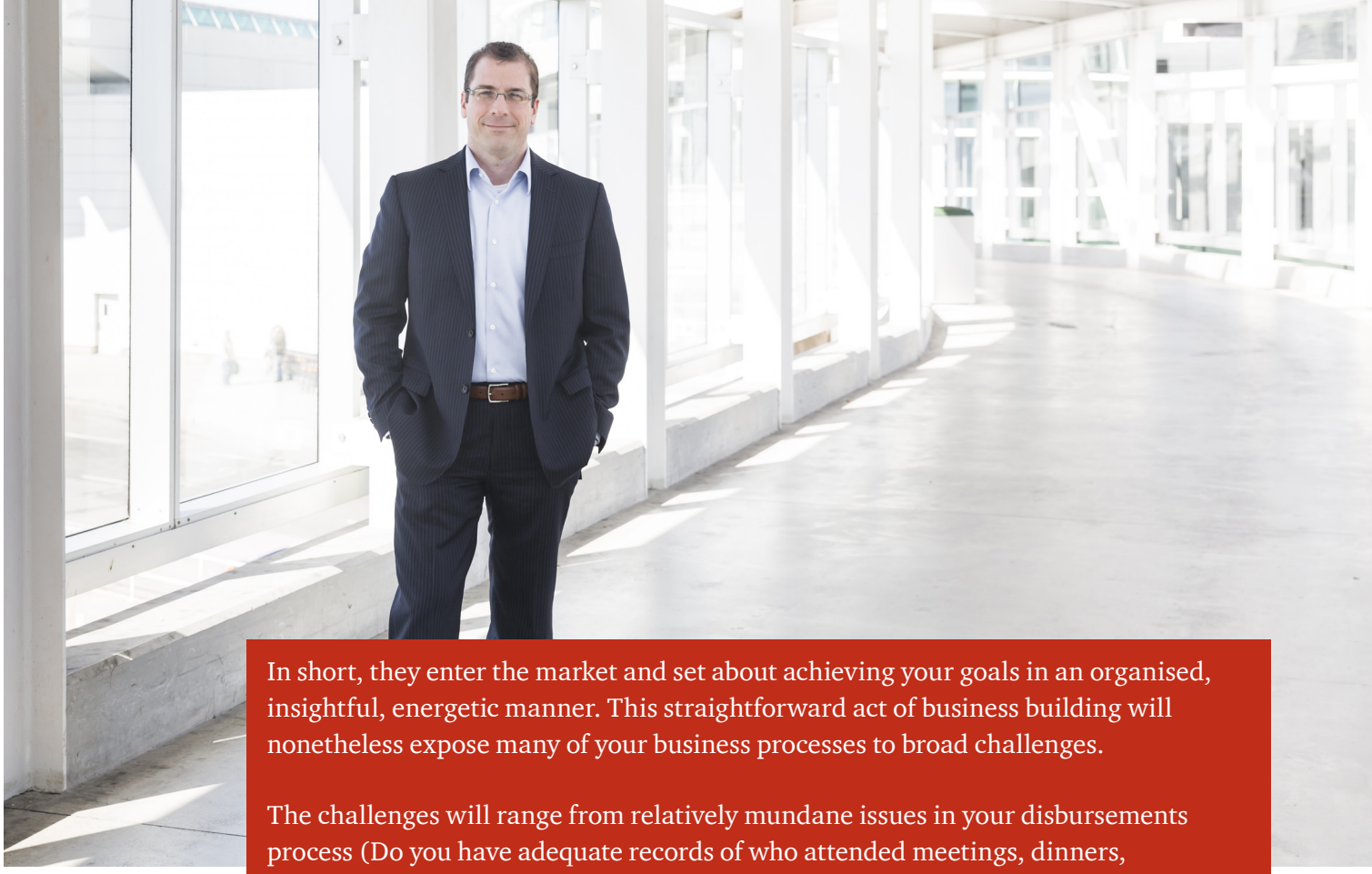
The number of respondents who reported incidences of money laundering in Zambia was 24% placing it as the fourth most prevalent economic crime experienced in the last 24 months in Zambia. This was against relatively low figures in Africa and Globally, at 12% and 11% respectively. In 2011, 9% of respondents reported incidences of money laundering at a Global level, an increase of 2% over the last 2 years. The next most prevalent form of economic crime and also quite new is cybercrime. These survey results indicate that cybercrime is a key concern for organisations with 22% of respondents in Zambia reporting cybercrime, 21% of Africa respondents and 24% of Global respondents reporting the same.

How corruption and bribery threaten your business processes

To highlight the threat that economic crimes of all types pose to numerous basic business processes, consider the following scenario, compiled from our portfolio of real-world experience.

A global company seeks growth in a culture where the risk of corruption is high. The company establishes a local sales force that puts in place an aggressive programme to market and sell to a wide spectrum of commercial, academic and government customers.

The sales force promptly engages the market with a series of meetings, events and demonstrations. They hire key staff with relationships with strategic buyers and influencers. They establish a distribution network after consulting with customers about their needs and expectations relative to logistical operations.



In short, they enter the market and set about achieving your goals in an organised, insightful, energetic manner. This straightforward act of business building will nonetheless expose many of your business processes to broad challenges.

The challenges will range from relatively mundane issues in your disbursements process (Do you have adequate records of who attended meetings, dinners, demonstrations and events? Did government officials participate? Were the value of the meals or any gifts exchanged within the bounds of corporate policy and local law?), to more complex issues concerning the business practices of your newly appointed distributors — and whether or not your due diligence process was adequate to identify potential issues, including whether or not you are dealing with government officials.

Meanwhile, your HR processes are challenged by the hiring of local staff with good connections in the marketplace — which may include relatives working as government officials at customer agencies. Your customs agent, conscious of the expectations that both you and your customers have placed on him for timely clearances, is entertaining local port officials on a regular basis. Your technical team has hired consultants recommended by the government and employed retired agency officials to assist with the approval and licensing processes for your products — again, challenging your due diligence process for vendor selection and your payment controls.

Your sales people are actively competing for business and are offering a few extra percentage points of discount to your distributors to win certain orders. Your law firm has placed a network of local labour attorneys on monthly retainer to deal with labour force issues. Finally, your tax team is engaged in a series of discussions with local tax authorities over the classification of your imports for customs duties, as well as your transfer pricing structure as it affects the profitability of your local subsidiary.

The reason we identify economic crimes as threatening your business processes is that none of the activities in the example above are per se improper or inappropriate. Still, each has the potential to challenge the integrity of your employees and pressure them as they struggle to manage the tensions of achieving your financial goals while operating in compliance with policy and regulation — in a local political and business culture characterised by a high demand for corrupt payments.

Financial loss is not the only concern that companies face when combating fraud.

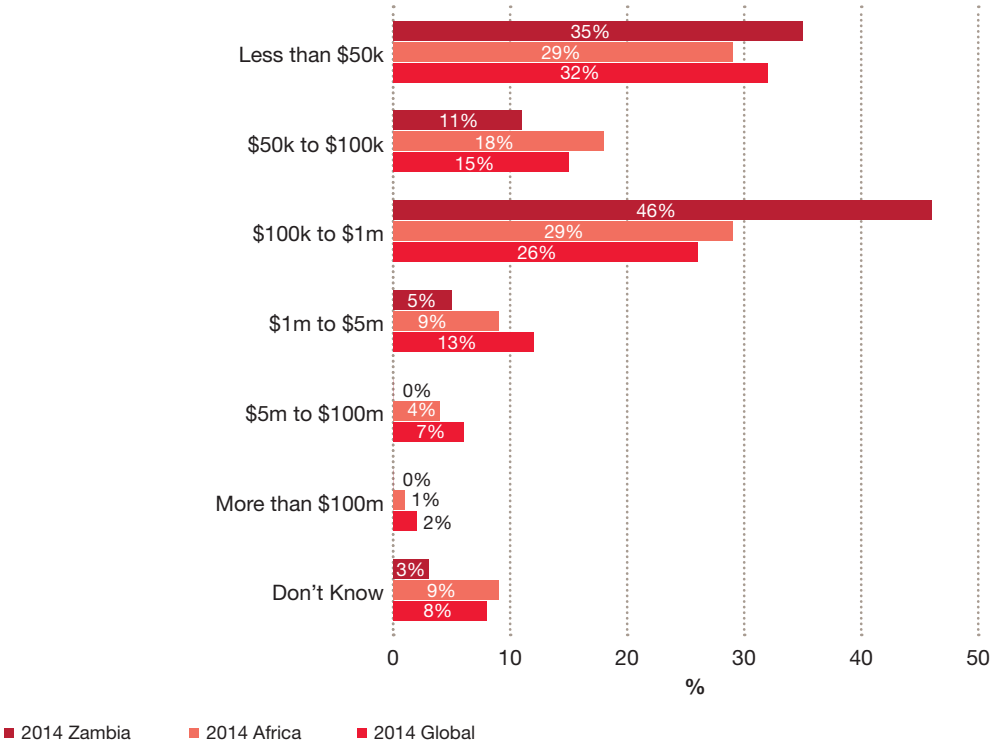
The damage

Organisations often don't grasp the true financial impact of an economic crime until after it has happened and sometimes well after. Our survey underscores that the cost of economic crime, both in financial and non-financial terms, is significant.

The Financial Damage: Rising Stakes

The cost of economic crime in Zambia is relatively high compared to Africa and Global levels. In this survey, almost half of the Zambian respondents, 46%, reported that the cost of economic crime suffered was between USD 100K and USD1m. In Africa 29% of respondents reported that they suffered less than USD 50K loss from economic crime which was less than the Global response where 32% reported the same.

Figure 3: Cost of Economic crime (in US$)

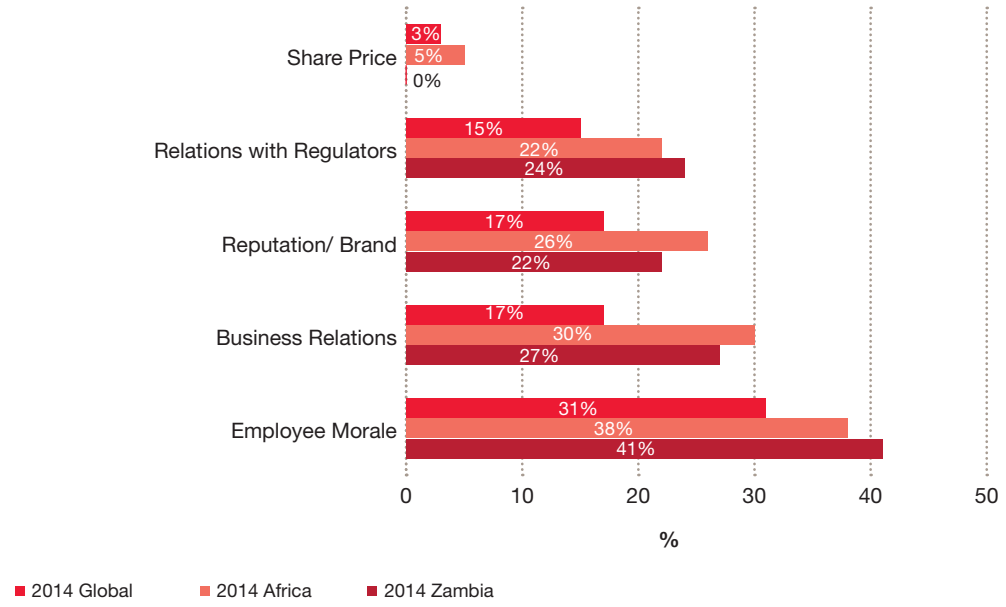


Collateral Damage: Hard to Quantify, Hard to ignore

Despite the high cost of economic crime, it does not appear to have significant effect on share price, reputation/ brand, or relations with regulators, as can be seen from the table above. However, compared to the results of the 2011 survey, there has been a 1% increase in the effect on organisation's share price from a global perspective over the last 2 years.

Economic loss is not the only concern that companies face when combating fraud. Our respondents pointed at damage to employee morale and business relations as some of the most severe non-financial impacts of economic crime.

Figure 4: Significant Fraud Impact on



The typical profile of the Zambian fraudster: 21 – 30 years of age, male with a university degree, holding a junior to middle management position.

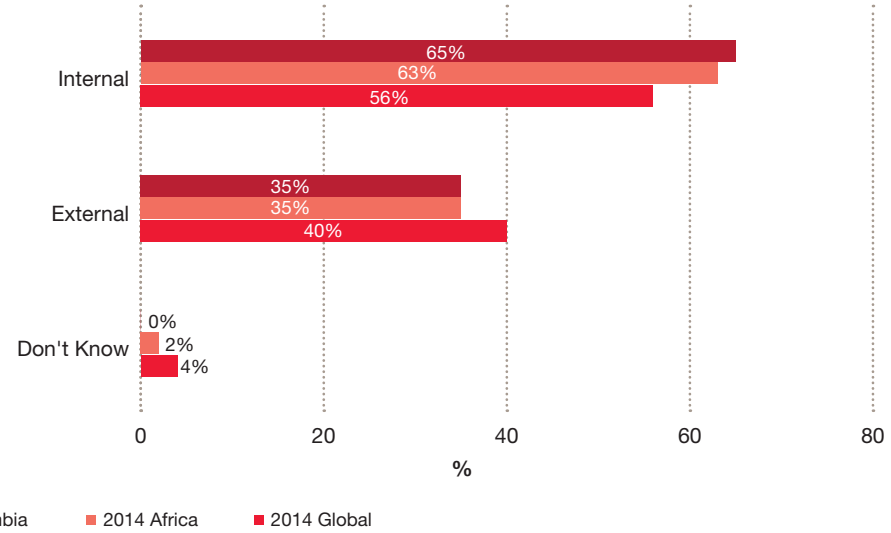
The Fraudster
Know your adversary

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

Of the three factors, opportunity is the one most within an organisation's control. This is a good thing. While life's pressures and the ability to rationalise may swirl around employees, if an organisation can limit the opportunity, they may be able to more often stop the fraud before it starts.

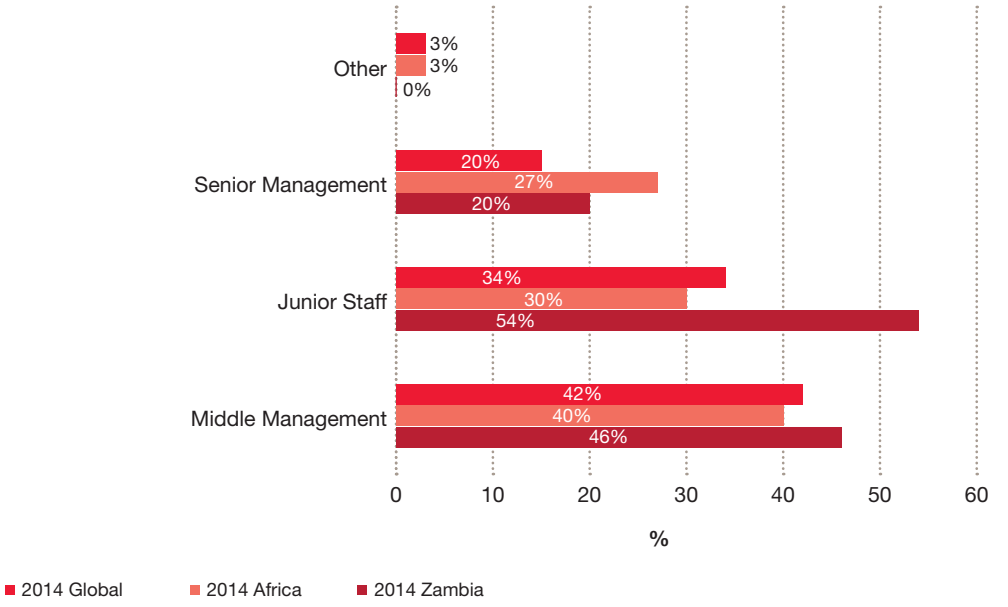
We asked respondents whose organisation experienced economic crime to profile the main perpetrator of the most serious fraud faced. The picture which emerged was that most fraud is committed by internal fraudsters, according to 65% of Zambian respondents compared to 63% in Africa and 56% Globally.

Figure 5: Major fruad perpetrator



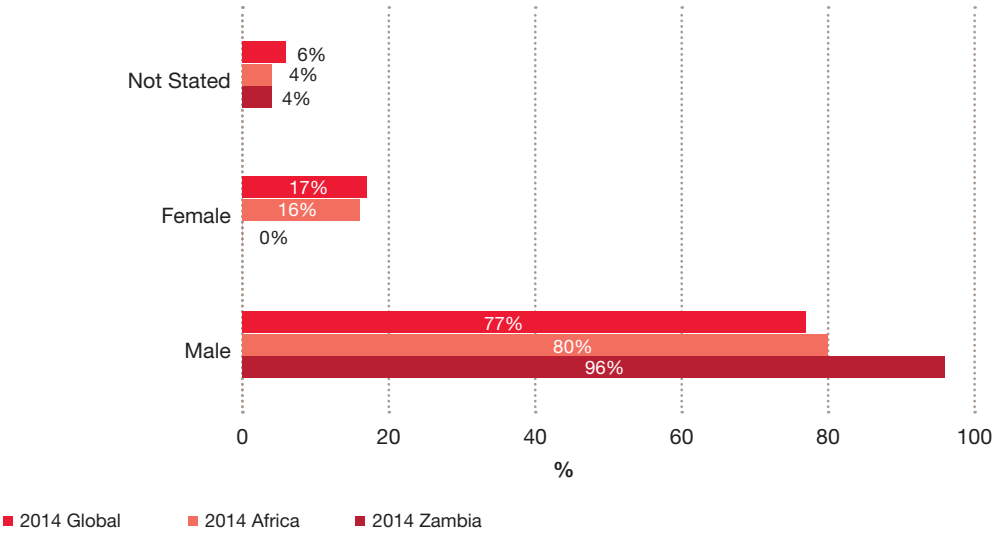
The most common perpetrators of fraud in Zambia are junior staff members (54%) and middle management (46%). The Africa and Global trends are that fraud is perpetrated first and foremost by middle management (40% in Africa and 42% Globally) followed by junior staff (31% in Africa and 34% Globally).

Figure 6: Level of internal fraudster



In addition it was noted that in Zambia, most fraudsters tend to be male (96%), between the ages of 21-30 years (46%), with a first degree (58%) and have served the organisation between 3-5 years (42%).

Figure 7: Internal fraud perpetrator by gender



The age of fraudsters differs slightly from the Africa and Global trends. In Africa and Globally, most fraudsters although male (80% and 77% respectively) are between 31-40 years (52% Africa and 39% Global) and have equally served the organisation between 3-5 years (37% Africa and 29%Global). Just like the local respondents, they also tend to have a first degree (Africa 48% and Globally 35%).

Figure 8: Internal fraud perpetrator by age

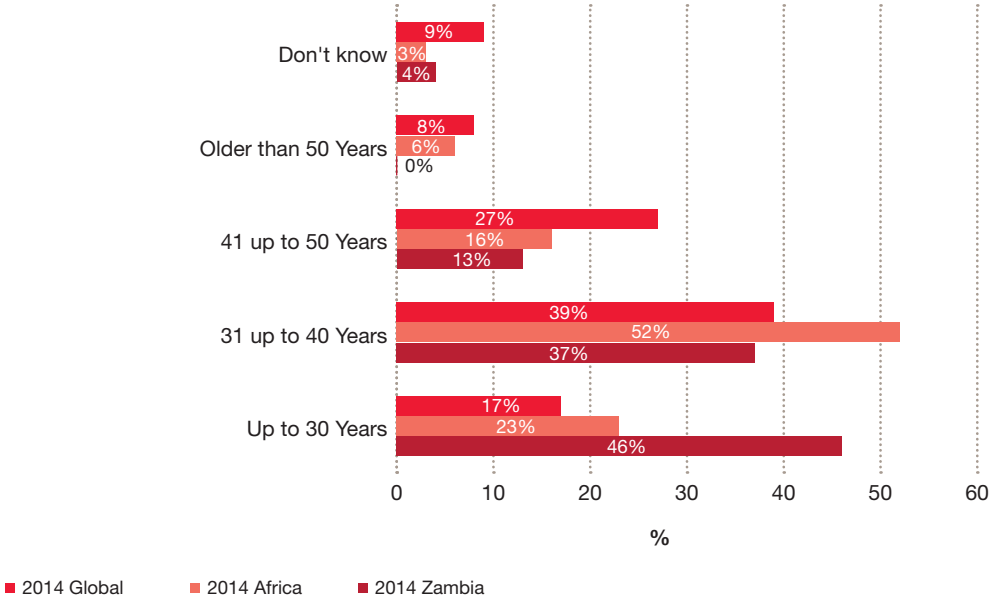
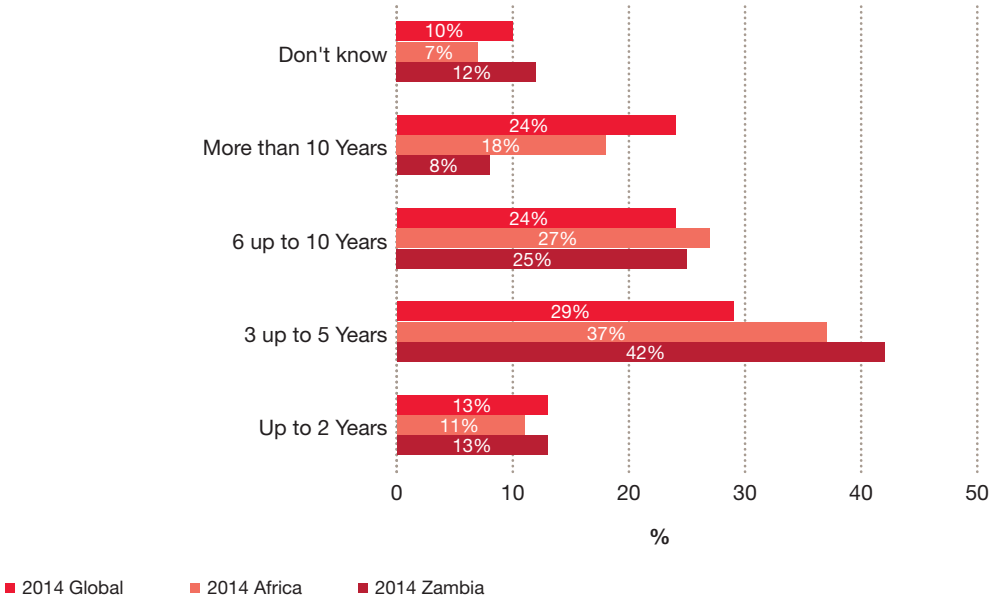
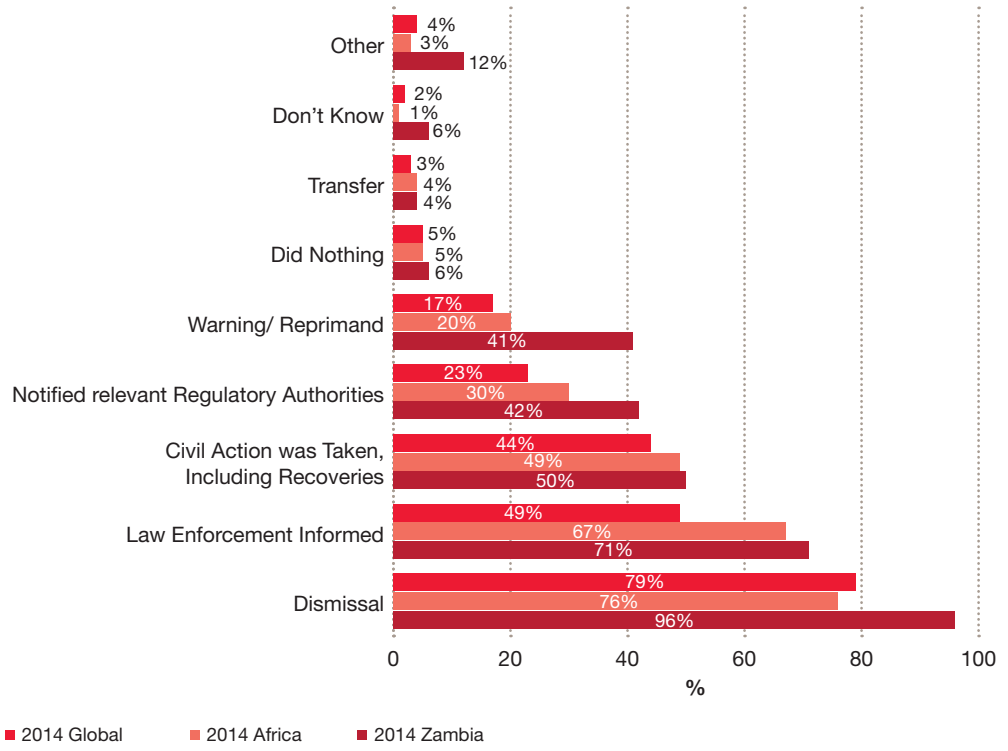


Figure 9: Length of service



When dealing with internal fraudsters most organisations prefer dismissing the perpetrator (96%) which mirrors the responses across Africa (76%) and Globally (79%). However, given the risks, it is somewhat concerning that 42% of Zambian organisations choose to merely issue a warning to the perpetrator, something that could indicate a casual attitude towards economic crime.

Figure 10: Actions Taken Against Internal Perpetrator



Senior Management and Fraud Impacts

In our experience, the age and seniority of the perpetrator of an internal act of fraud have a proportionately large effect on its impact. That's because executives of greater seniority are likely to get a greater degree of deference in navigating exceptions to internal control policies.

Consider the senior private banker who assures the wire transfer operators that he'll handle the client call-back procedure to confirm instructions for payments. Or the boss who says she'll take care of getting the documentation needed to support the payment. Or even the division manager who budgets a the amount he intends to "withdraw" from the corporate coffers based on bogus invoices for services.

These real-life examples illustrate the unique position of senior people. Not only are they authority figures with respect to internal control policies — and thus have access not enjoyed by employees of lesser rank — they can also be custodians of the corporate culture. As such, the financial damage of the fraud can be compounded by its corrosive effect on that same culture.

This also compares unfavorably with Africa (20%) and Globally (17%). These findings suggest that organisations in Zambia may need to take a more serious approach to dealing with economic crime so as to act as a deterrent against those considering such acts and to set the tone that fraud will not be tolerated at any level.

Among external fraudsters, the chief perpetrators of fraud are neither vendors nor agents/ intermediaries. This trend differs from the Africa and global trends. In Africa, 33% of respondents attributed chief perpetration of fraud to agents/intermediaries. Globally, the chief perpetrators of fraud are thought to be customers (32%). This could be because of changes in business models where more processes are being outsourced as opposed to being undertaken internally, thereby creating more potential for fraud.

On the other hand, the procurement process appears to be the area most affected by fraud. 64% of Zambian respondents reported that fraud was most frequently committed during the process of vendor contracting/maintenance. This is especially true in the tendering process for government bids where a number of accusations of corruption have been made.

Figure 11: External Fraudster

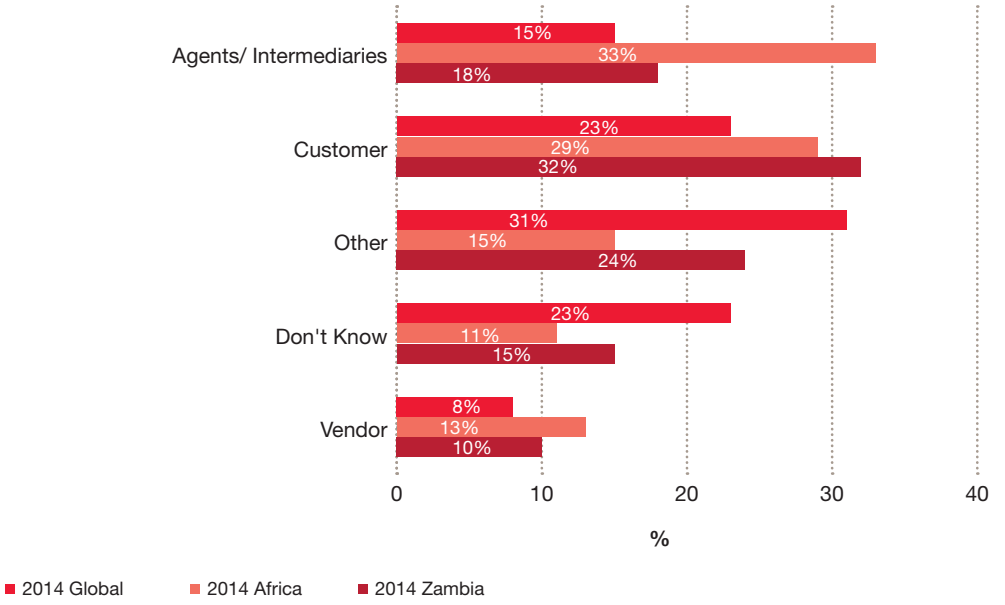
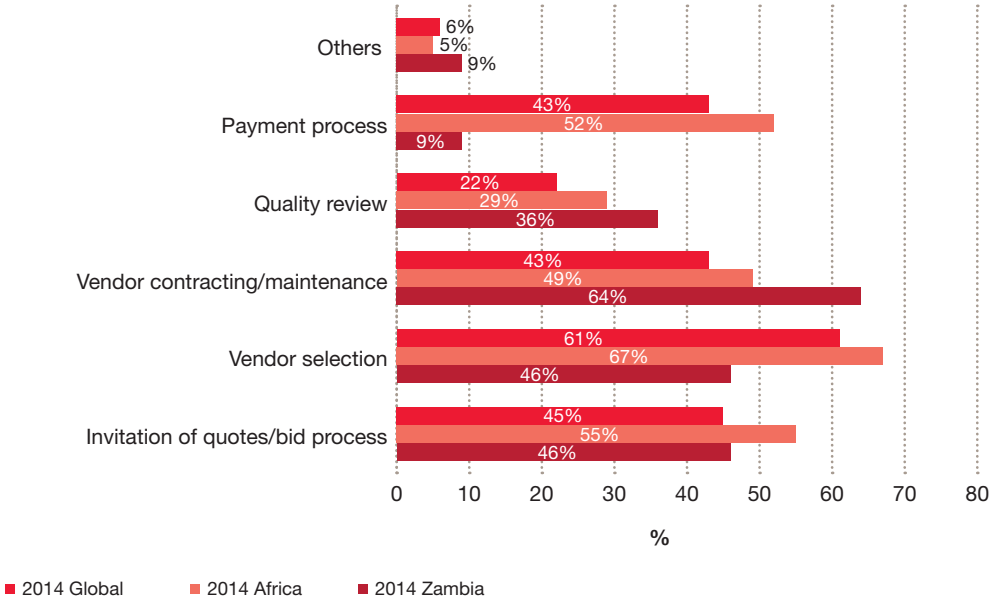


Figure 12: Procurement fraud occurence



Many factors can be attributed to this, one of them being the high value of the bids in the public sector. For instance, according to the Report of the Auditor General on the Accounts of Zambia for the financial year ended 31 December 2012, payments amounting to ZMW121,438,503 in respect of goods and services procured during 2012 were processed without following procurement procedures. The Report states that this is a result of the failure to adhere to regulations and weaknesses in the implementation of internal control systems.

When taking action against external fraudsters, most organisations in Zambia (69%) prefer to contact law enforcement agencies, similar to the results for Africa (59%) and Globally (61%).

In Zambia 55% of respondents uncovered fraud through internal controls - data analytics (16%) and reporting of suspicious transactions (14%) were the most common detection methods.

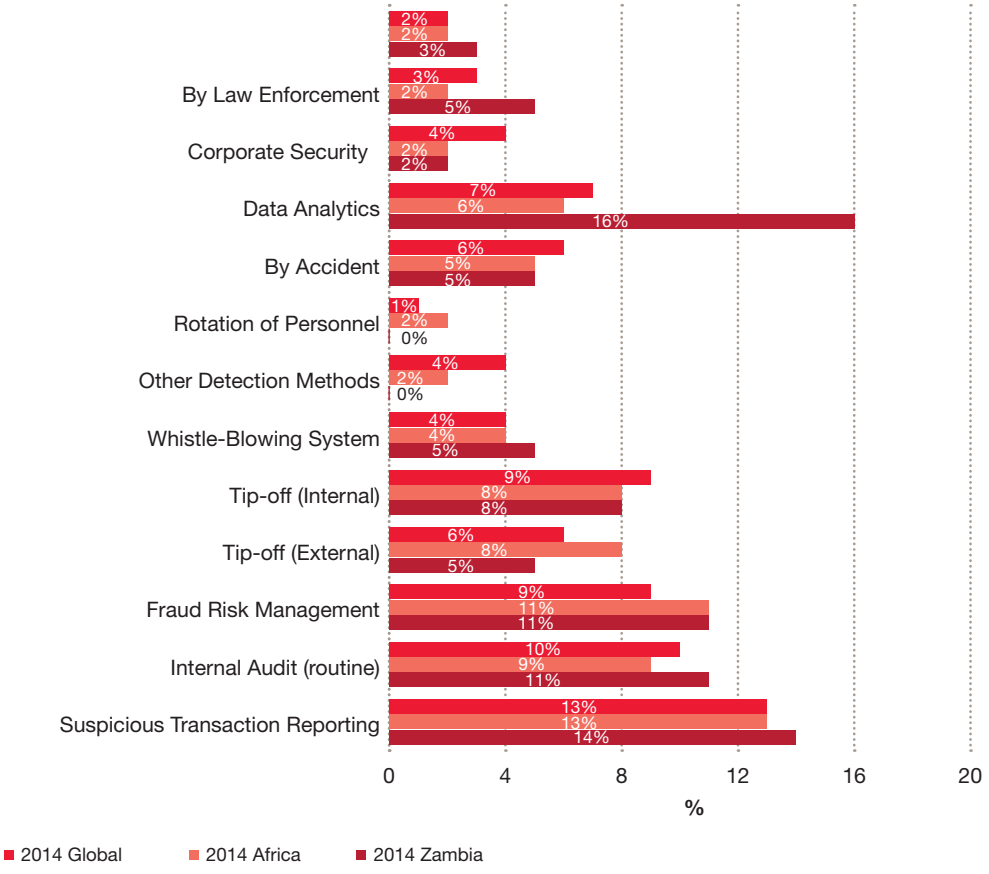
To catch a thief

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

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

In Zambia, the most effective methods of detecting economic crime are data analytics (16%), and suspicious transaction reporting (14%) which is also true in Africa (13%) and Globally (13%). Routine internal audit and fraud risk management were also common methods of crime detection and accounted for 11% each. The graph below compares the different methods of fraud detection used by organisations in Zambia, Africa and Globally.

Figure 13: Detection of Fraud



Rise of Data Analytics

Over the past several years, we have seen a marked rise in the number of major frauds discovered through data analytics and suspicious transaction reporting. What does this process entail?

Data analytics begins with a systematic approach to data gathering, cleansing, and standardisation. Current technology enables analytics to leverage a growing abundance of available and disparate information, allowing for better comprehension of an organisation's data — and therefore a better understanding of potential risks.

A well-designed programme will efficiently risk-rank transactions and entities for investigation, and may use an approach which facilitates the detection of hidden relationships and connections with known high-risk entities. It identifies atypical transactional patterns through statistical, keyword, and exception-based data mining.

Through continuous feedback, anticorruption and antifraud analytics continue to evolve and improve. Companies are implementing frameworks and optimizing findings by leveraging their collective knowledge and experiences from past reviews and investigations.

Moving forward, we expect more organisations to build on this success story, and use these leading data analysis tools to help detect and mitigate fraud.

Greater awareness of how fraud is detected can help organisations tailor their procedures to increase effectiveness. It appears that one of themes from the early years of the global survey — that successful mitigation of future fraud starts with understanding past and current threats — is taking root.

One of the ways of identifying fraudulent activities in organisations is through a fraud risk assessment. Over 70% of organisations in Zambia have conducted a fraud risk assessment at least once in the last two years.

This is a good statistic as it highlights the seriousness of businesses to identify fraud and possibly avoid it. Despite this it is surprising that 12% of organisations in Zambia do not conduct fraud risk assessments at all. Yet another surprising finding is that 40% of Zambian respondents do not know what a fraud risk assessment is, while 20% of respondents believe that a fraud risk assessment is either not necessary or is too costly.

These statistics tally with Africa and Global figures where 37% in Africa and 30% Globally attributed their lack of conducting a fraud risk assessment due to the fact that they do not know what it actually entails. Further, 24% of Africa respondents and 30% of global respondents did not perceive the value of such assessments.

Figure 14: Frequency of fraud risk assessments performances

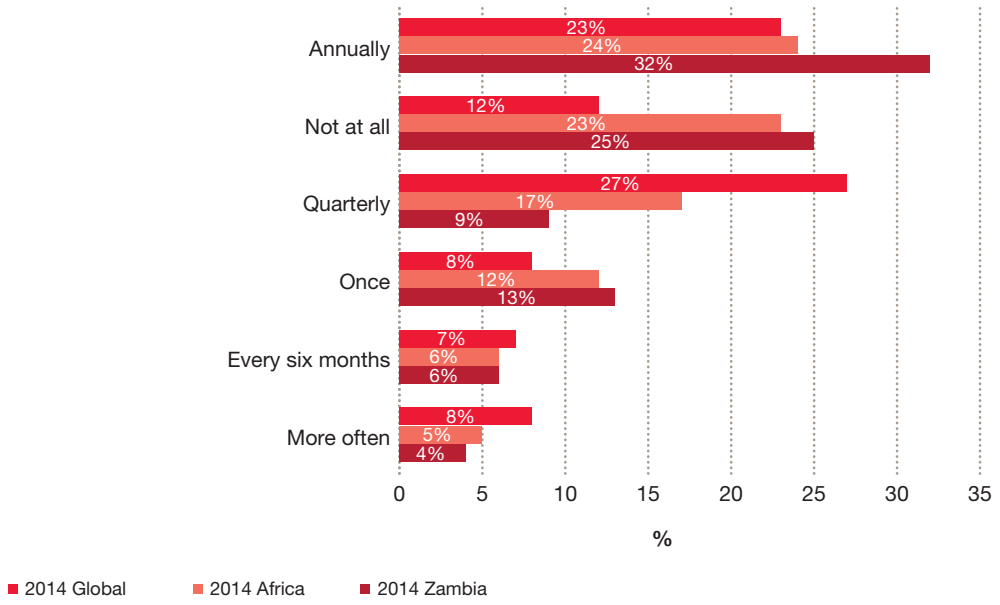
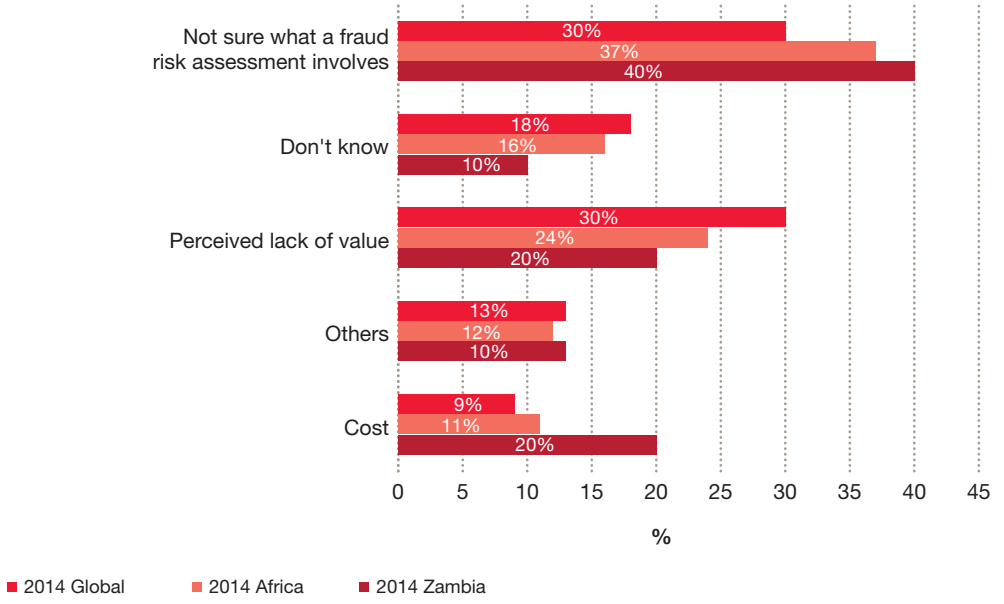


Figure 15: Reason for not performing a Fraud Risk Assessment



Although the estimated financial loss of cybercrime in Zambia is relatively low, the threat of reputational damage, service disruption and theft/loss of data is a major concern to the majority of respondents.

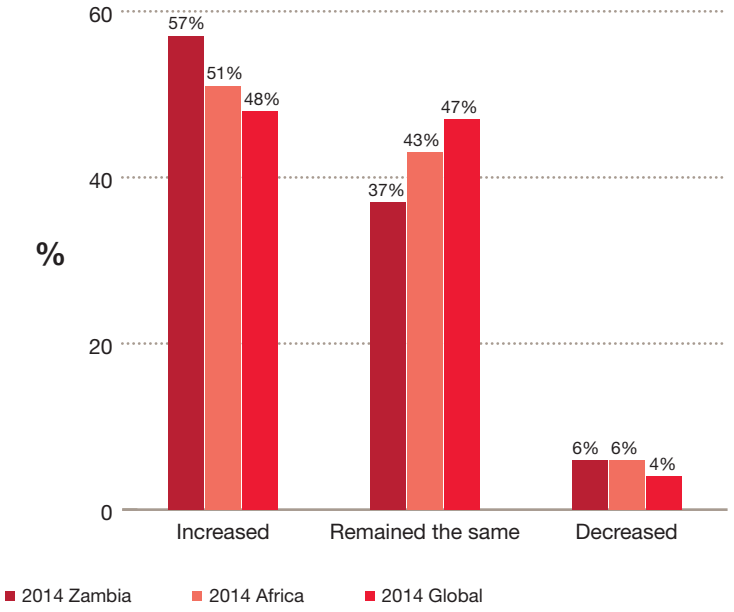
Cybercrime
The risks of a networked world

The advancement of technology in business services, combined with the explosive growth in social media and data connectivity, has permanently altered — and in many ways, brought together — the business and consumer landscapes.

Unfortunately, connectivity and access also have a dark side — one which empowers motivated, sophisticated criminals who are able to operate below the radar. And because cybercrime operates largely unseen, organisations may never even realise they are being targeted until long after the damage is done.

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

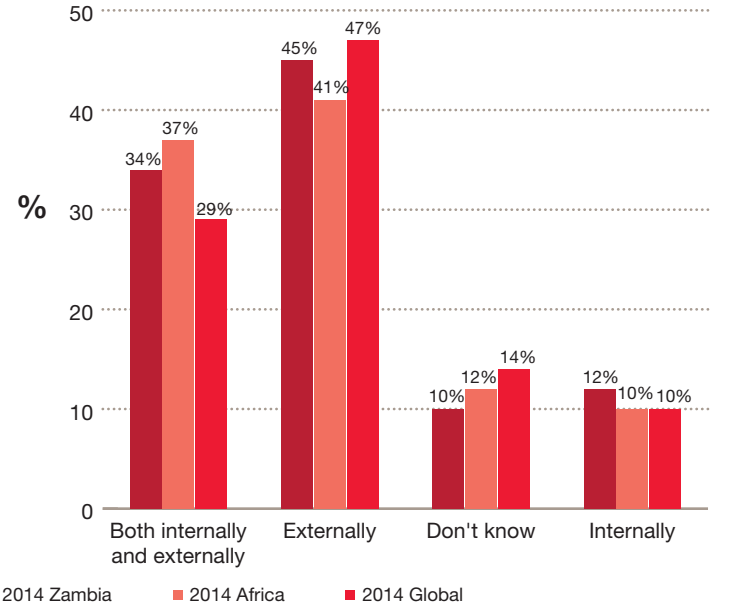
Figure 16: How perception of risk of cybercrime has changed



Cybercrime: What You Don't Know Can Hurt You

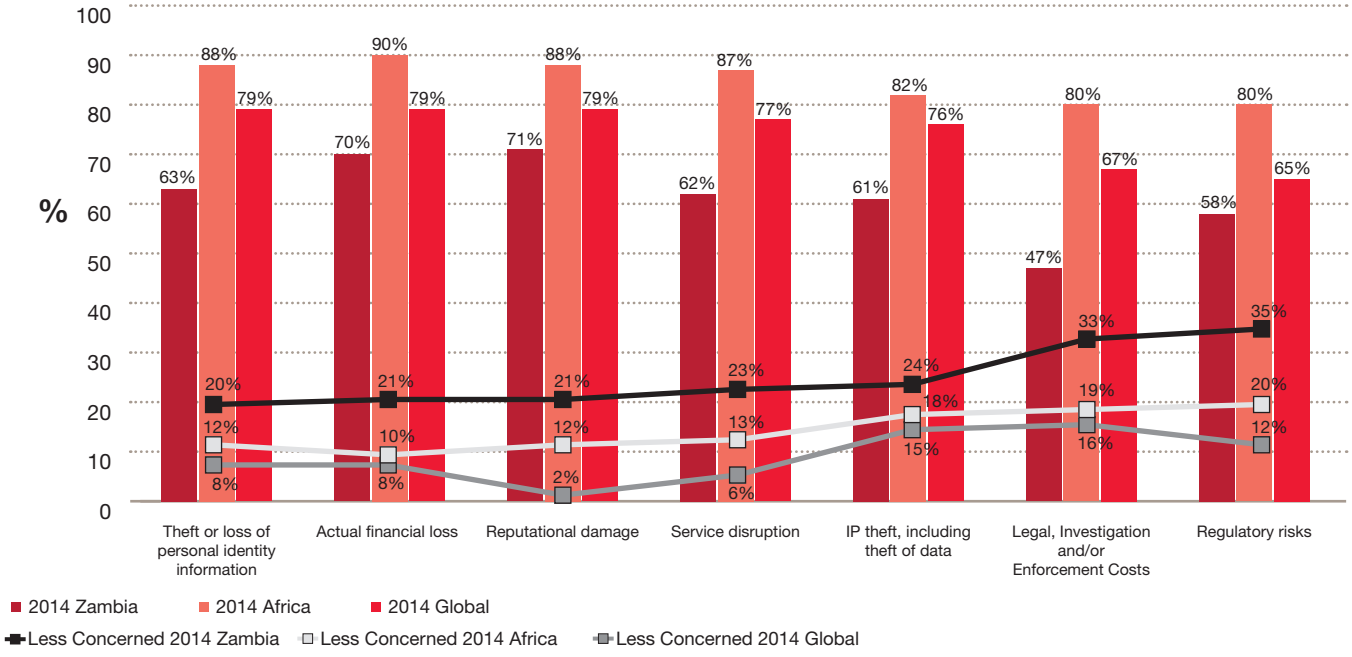
Around 57% of Zambia respondents indicated an increased awareness to incidences of cybercrime, while Africa had 51% and Globally 48% reported the same. This could be as a result of greater media coverage and advances in technology. There has been greater coverage of incidences of ATM pin theft and internet fraud in the media.

Figure 17: Greatest Threat of Cybercrime



Most Zambia respondents (45%) believe cybercrime is perpetrated by external sources, while 41% of Africa and 47% of Global respondents reported the same. However, a good number of respondents in Zambia (34%) believe that cybercrime is perpetrated by both internal and external sources. This is in line with the Africa (37%) and Global (29%) responses.

Figure 18: Concerned about effects of cybercrime activity

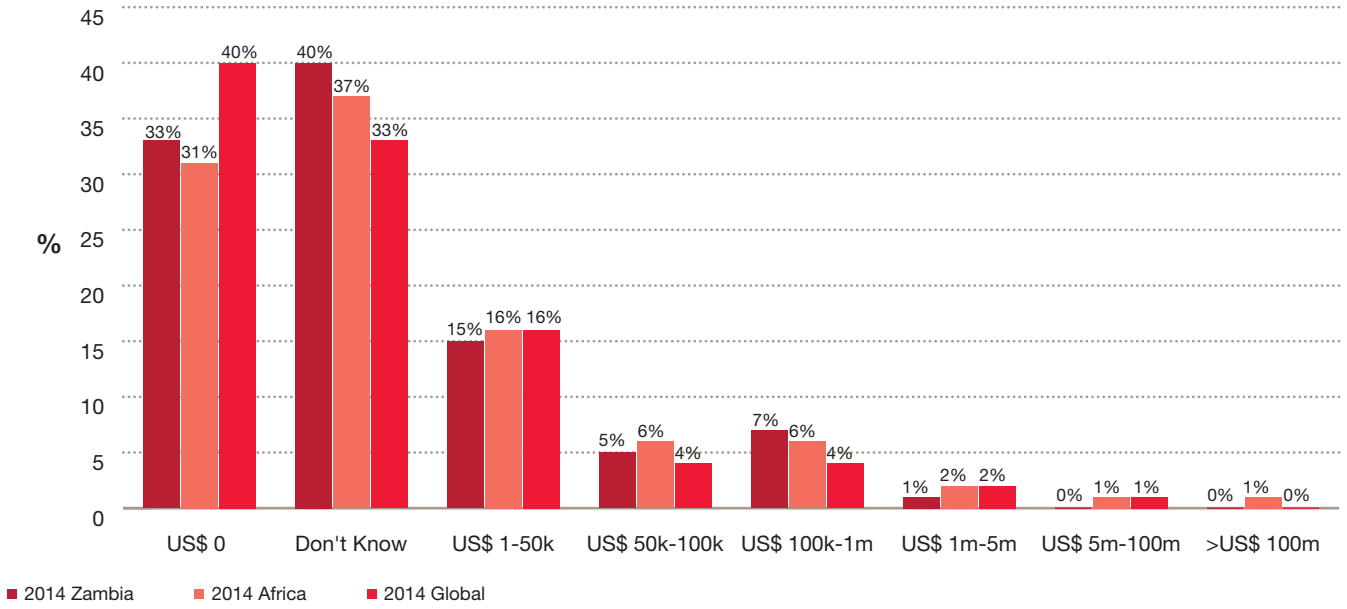


Of all potential effects of cybercrime, the one perceived to be most severe according to Zambian respondents is reputational damage with 71% reporting this. In Africa, 61% and Globally 41% reported the same. On a country level, actual financial loss, theft/loss of personal identity information and reputational damage account for 70%, 63% and 71% respectively. This trend is different in Africa, with actual financial loss accounting for 59% of the responses. This is followed by theft/loss of personal identity information (57%) and reputational damage.

What is alarming is the lack of knowledge on the financial impact of cybercrime, this can be seen in the graph above. Despite the high perception of cybercrime, the vast majority of respondents did not know how much their company has lost as a result of cybercrime (40%). This trend is mirrored on continental level (37%) as well as at a Global level (33%).

This underscores the challenge of the threat. Many entities do not have clear insight into whether their networks and data contained therein have been breached, and they don't know what has been lost, or its value.

Figure 19: Estimate cost of Cybercrime



Cybercrime threatens technology-enabled business processes

The growing use of technology-enabled business processes makes cybercrime a very real threat to a wide variety of business operations. In our recent experience, the systems most threatened are those that contain data directly leading to financial assets that can be stolen, or personal data that can be used to assemble an attack on financial assets.

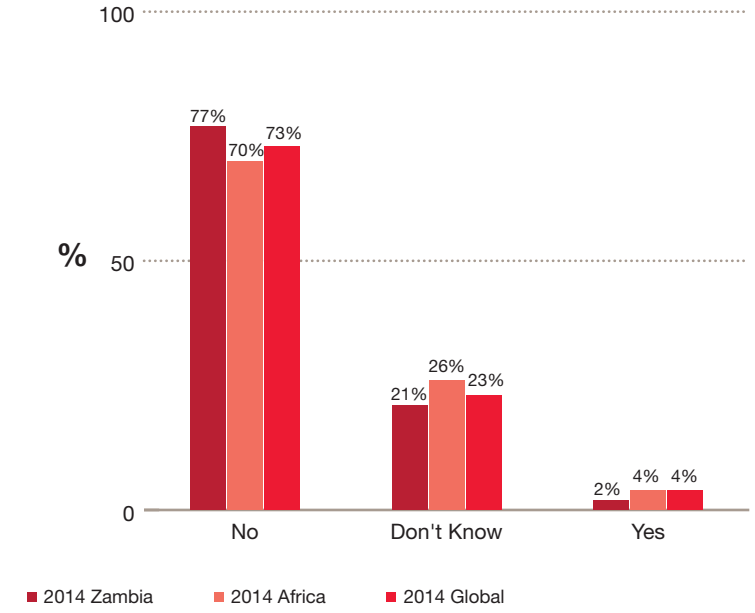
The technology-enabled business processes that are threatened by cybercrime include:

- **Point of sale purchases** by debit and credit cards in the everyday retail environment.
- **ATM transactions** in the everyday banking environment.
- Preserving or respecting the **privacy of customers.** This is especially true in the health care industry, where providers often maintain systems with considerable amounts of sensitive patient information, including identity, financial circumstances, insurance plans, and medical condition.
- **E-commerce or on-line sales processes.** Same issues as penetration of point of sales systems in the retail store or banking environment, except that it is in the on-line environment.
- **Electronic business communications (email).** External cyber criminals can penetrate corporate communications systems and steal critical commercial information, intellectual property, and sensitive executive communications.
- Taking advantage of **infrastructure weak points** to accomplish any of the above — for example, penetrating Wifi access points or intercepting other people's communications through them; attacking business operating systems using a "cloud" architecture by penetrating the server environment maintained by the cloud provider.

Social Media and Cybercrime

Social Media sites such as facebook and twitter have played an important role in making it easier to stay in touch with friends, loved ones and even business associates. However, with this connectivity, the risk of cybercrimes has also increased. Interestingly enough, most respondents in Zambia, Africa and the World have not experienced cybercrimes due to exposure to social media such as facebook and twitter.

Figure 20: Social Media & Cybercrime

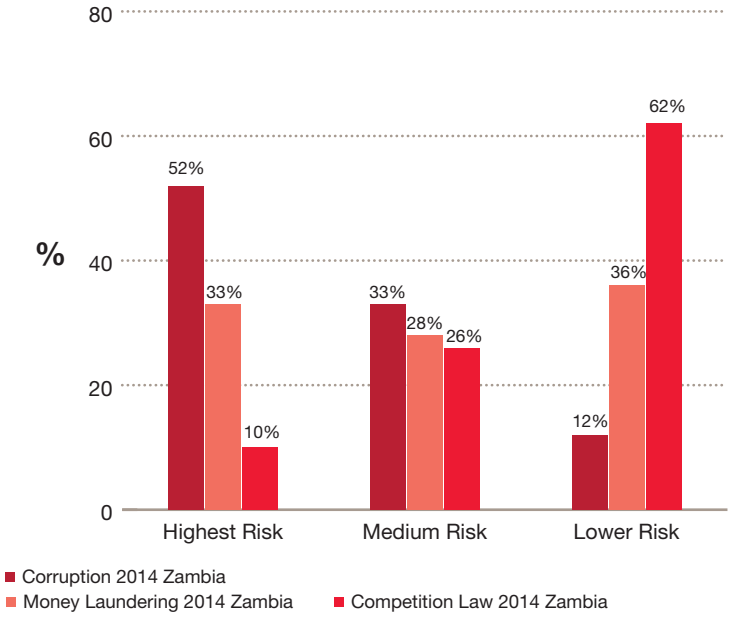


In the past 2 years, although the majority of organisations (41%) have never been asked to pay a bribe, the perception of corruption levels in Zambia is high (52%).

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

The highest perception risks of economic crime are the prevalence of corruption in Zambia. The majority of Zambia respondents perceive this economic crime to be the highest risk, which is mirrored by the high prevalence of corruption in Zambia. Medium high risk crime in Zambia was money laundering while competition law/ anti trust law was viewed to be the least risky.

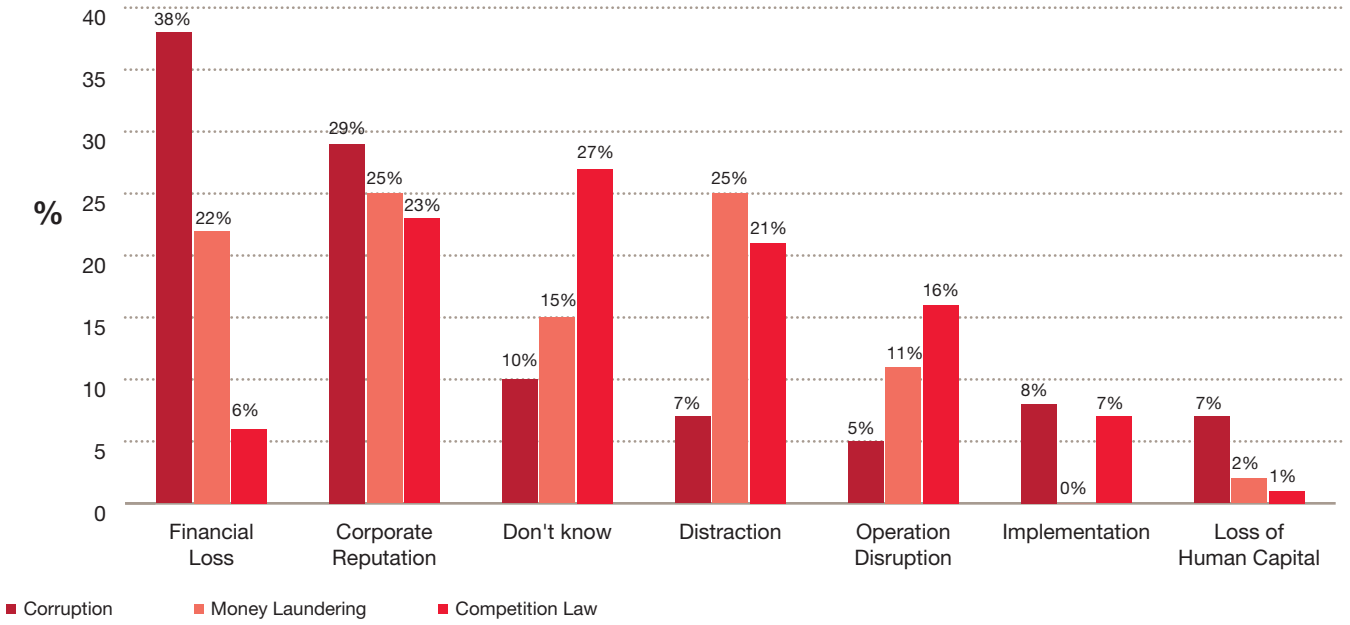
Figure 21: Risk perception



The most severe impacts caused by these economic crimes can be seen in the table below. Corruption accounted for the greatest financial loss (38%) followed by corporate reputational damage (29%).

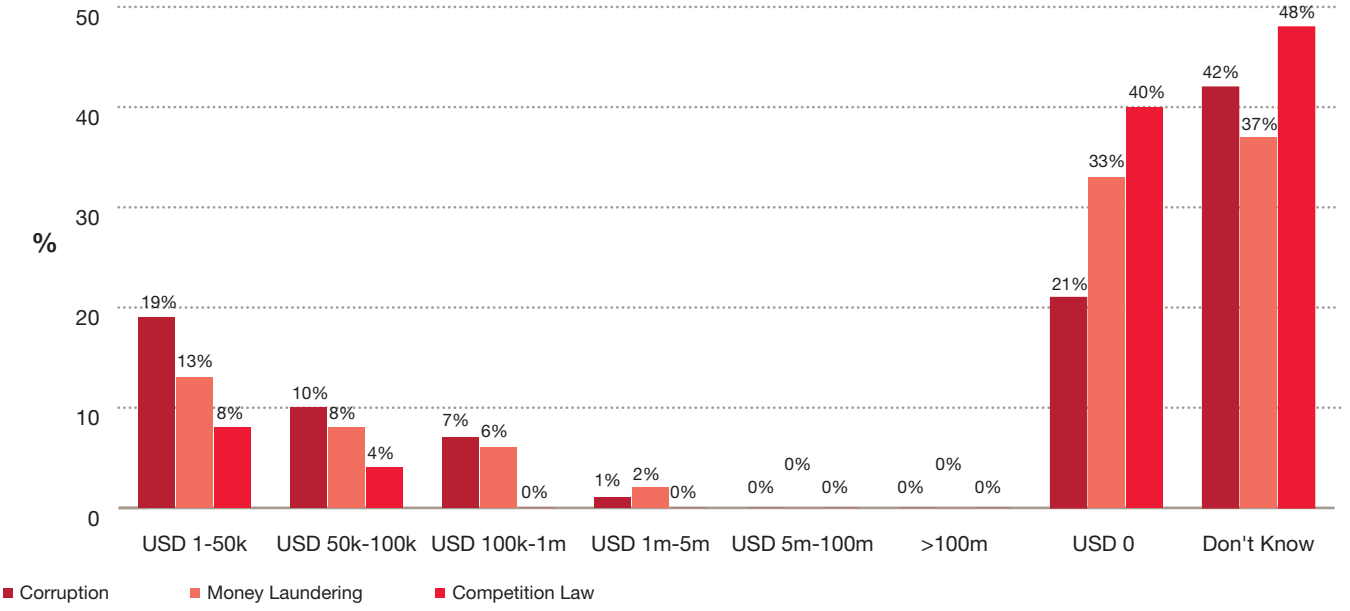
Money laundering on the other hand, is perceived to have the greatest impact on corporate reputational damage and distraction with 25% reporting these trends.

Figure 22: Most Severe Impact to organisations in Zambia



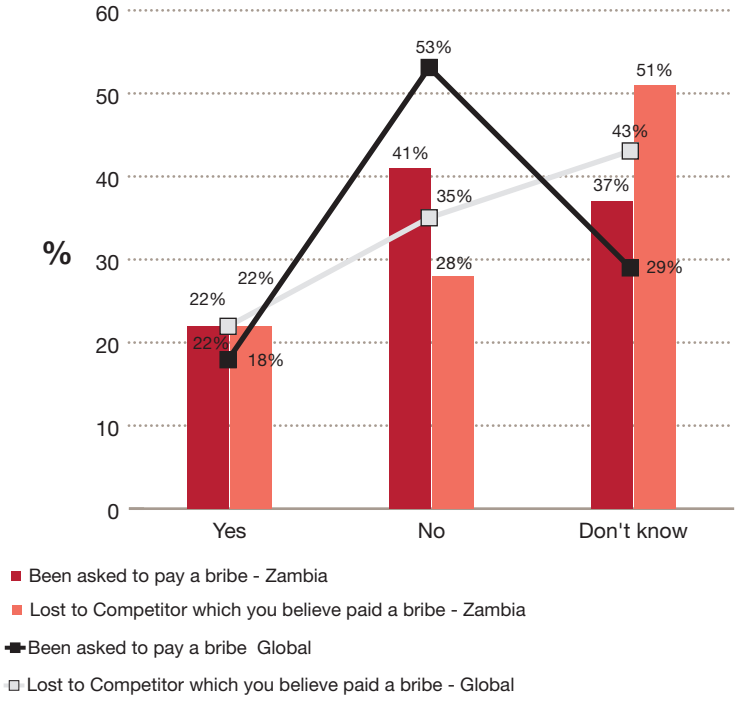
Again, surprisingly, although the vast majority of respondents indicated that corruption (42%), money laundering (37%) and competition law/anti trust law (48%) are serious crimes, most respondents do not know the monetary loss from these crimes.

Figure 23: Loss through incident types in Zambia



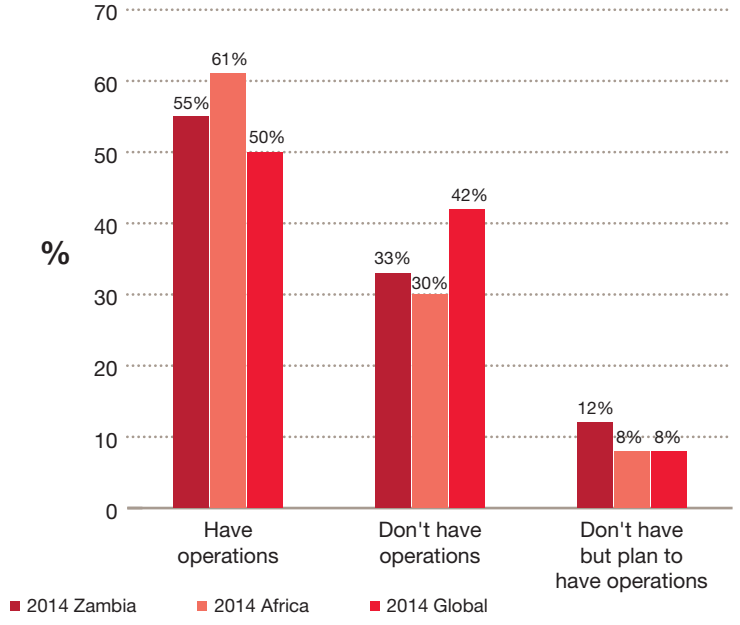
Despite high incidences of corruption in Zambia, in the past 24 months the majority of organisations (41%) have never been asked to pay a bribe, 37% do not know whether their organisation has been asked while 22% were asked to pay a bribe. 22%of the respondents believe they lost to a competitor who paid a bribe while 28% believe that they just lost. On a Global level, 18% were asked to pay a bribe, 53% were not asked, and 29% of respondents do not know. As for losing an opportunity to a competitor who paid a bribe, Globally 22% say they lost the opportunity in this way, 35% did not, while 43% do not know. This can be seen in the graph below.

Figure 24: Has your organisation



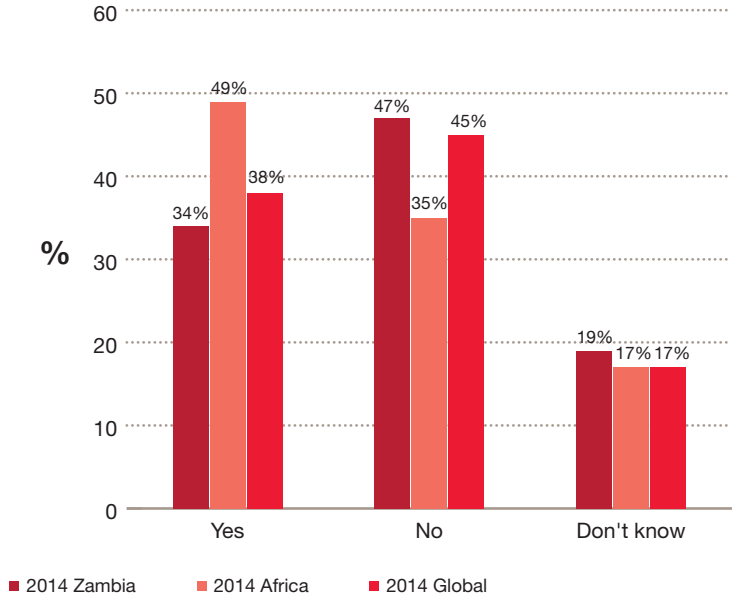
Despite the threats of corruption, more than half of the organisations in Zambia, Africa and the World have operations in high level corruption markets. In Zambia 55%, Africa 61% and Globally 50% have operations in territories identified as posing a high corruption risk and 12% of the respondents plan to open operations in these territories in the next 24 months.

Figure 25: Operations in High Level Corruption Markets



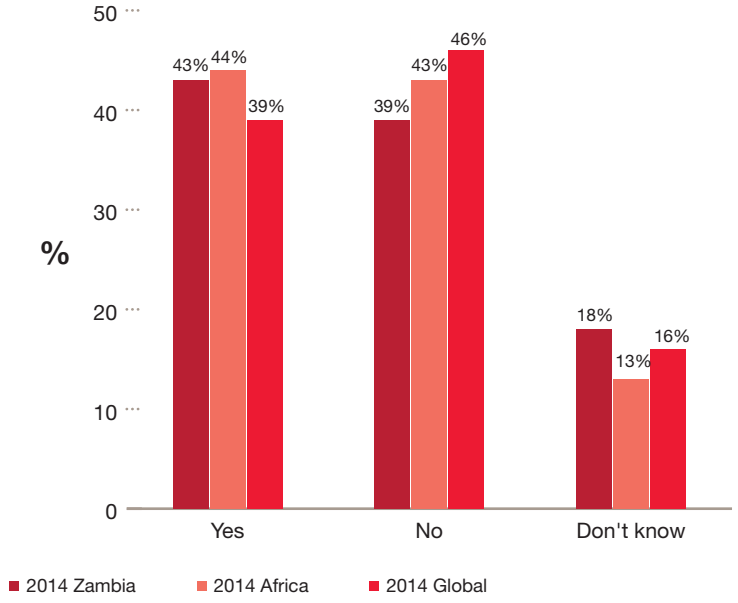
As illustrated by the graph below, our respondents, 34% of Zambia, 49% Africa and 38% Globally indicated that their organisations are pursuing opportunities in markets with high levels of corruption.

Figure 26: Pursuit of opportunities in markets with high level of corruption



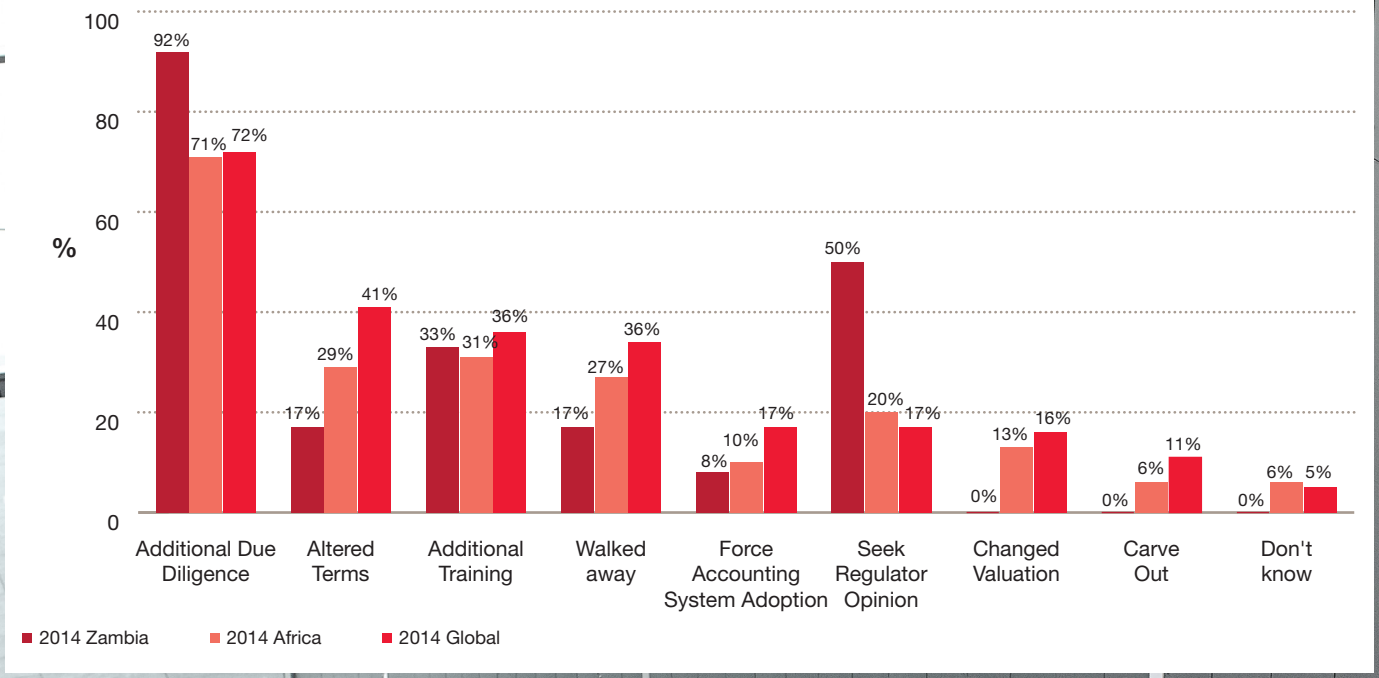
As shown by the results displayed below, despite 43% of our respondents in Zambia indicating that the potential corruption risk altered their business plan or strategy 39% of the respondents did not alter their business plan or strategy.

Figure 27: Altered pursuit of opportunities in markets with high level of corruption



When asked how they altered their business plan/strategy, 17% of our respondents walked away from the business opportunity because of the corruption risk. The majority of our respondents (92%) opted to perform additional due diligence procedures, which responses mirror Africa (71%) and Global (72%) while 50% opted to seek an opinion from the Regulator in anticipation of the potential acquisition and 33% decided to provide additional training to targets employees.

Figure 28: How organisation altered pursuit of opportunities in markets with high level of corruption



It is easy for those who have lived in relatively corrupt free societies to underestimate the significance and power of cultural norms related to the demand side of corruption.

Bribery and corruption
The global perspective

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

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

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

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

Conclusion

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

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

Fraud prevention measures will also be key in acting as a deterrent and in the detection of economic crime. The responses from our survey indicate that a lot more can be done in combating economic crime.

Taking a proactive approach to economic crime is critical. Apart from the measurable financial losses, we must take into account the wider impact. A bold approach to tackling economic crime in today's world is not an option – it's an imperative.

Methodology

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

The survey had four sections:

- general profiling questions
- comparative questions looking at what economic crime organisations had experienced
- cybercrime fraud threats
- corruption/bribery, money laundering and competition law/antitrust law

About the survey

The 2014 Global Economic Crime Survey was completed by 5,128 respondents (compared to 3,877 respondents in 2011) from 99 countries (compared to 78 countries in 2011). Of the total number of respondents, 50% were senior executives of their respective organisations, 35% represented listed companies and 54% represented organisations with more than 1,000 employees.

We used the following research techniques:

- Survey of executives in the organisation. The findings in this survey come from executives' reports of their experiences of economic crimes in their organisations. We obtained information from them on the different types of economic crime, their impact on the organization (both the financial loss and any collateral damage), the perpetrator of these crimes, what action the organisation took and how they responded to the crime.
- Questions relating to cybercrime, corruption/bribery, money laundering and competition law/antitrust law. This survey takes a detailed look at these threats which are often systemic in nature and thus are more prone to have a long term, damaging impact on the organisation.
- **Analysis of trends over time.** Since we started doing these surveys in 2001, we have asked a number of core questions, and extra ones that are relevant from time to time, dealing with issues likely to have an impact on organisations around the world. With this historical data to hand, we can see current themes, chart developments, and find trends.

Terminology

Accounting fraud

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

Asset misappropriation, including embezzlement/deception by employees

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

Bribery and Corruption

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

Competition Law/Antitrust Law

Law that promotes or maintains market competition by regulating anticompetitive and unfair business practices conduct by organisations. Examples may include price fixing, excessive, predatory or discriminatory pricing, unfair trading terms, and tying (i.e., stipulating that a buyer wishing to purchase one product must also purchase all or some of his requirements for a second product).

Cybercrime

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

Economic crime

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

Espionage

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

Financial loss/Financial terms

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

Fraud risk assessment

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

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

Human Resources fraud (recruitment and/or payroll fraud)

Fraud committed by members of the Human Resources department, including payroll fraud, ghost employees, pay-to-work, recruitment (i.e., hiring friends and/or relatives, hiring unqualified individuals, falsification of documents, etc.).

Incentive/Pressure to Perform

The individual has some financial problem that he/she is unable to solve through legitimate means so he/she begins to consider committing an illegal act as a way to solve the problem. The financial problem can be professional (e.g., job is in jeopardy) or personal (e.g., personal debt).

Insider trading

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

IP infringement (including trademarks, patents, counterfeit products and services)

This includes the illegal copying and/or distribution of fake goods in breach of patent or copyright, and the creation of false currency notes and coins with the intention of passing them off as genuine.

Markets with a high level of corruption risk

While corruption risk levels can be subjective, for the purposes of this survey we suggest a territory with a 2012 Transparency International Corruption Perception Index ("CPI") score of 50 or less be considered a market with a high level of corruption risk.

Money laundering

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

Mortgage Fraud

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

Opportunity or ability

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

Procurement Fraud

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

Rationalisation

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

Tax Fraud

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

www.pwc.com/zm

Designed by PwC Design Studio (JB 14-14792)