Adjusting the Lens on Economic Crime

Preparation brings opportunity back into focus

61%

Of respondents reported having suffered an economic crime in the last two years.

72%

Of respondents cited Asset Misappropriation as the most common economic crime committed in organizations in Kenya.

26%

Of respondents reported that there was no incident response plan for cyber-attacks in their organization and neither was there plans to implement one.

pwc

Contents

3 *Foreword*

4 *Introduction*

5 *Economic Crime in Kenya*

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

11 *Special focus on cybercrime and money laundering in Kenya*

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

16 *Conclusion*

17 *Contacts*

18 *Participation statistics*

Foreword

The last 2 years have been tough on the Kenyan economy. Despite the fall in crude oil prices which are traditional triggers for improved productivity and stability of the Kenya Shilling, the country (and the world) has seen a rallying of the US dollar and a slow-down of the Chinese and other emerging economies.

The Kenya Shilling has struggled against the global currencies falling from an exchange rate of about KShs 86 against the dollar in February 2014 to the current average of KShs 102[1]. The Central Bank of Kenya has gone to great lengths to try and stabilise the Kenya Shilling without adversely affecting the economy. While the exchange rate has been unfavourable to the Kenya Shilling, inflation has been managed at between 6.9% in 2014 and 6.6% in 2015[2].

In the last two years, the NSE 20 Share index has risen from 4,933 points in February 2014, to a high of 5,491 points in February 2015 before shrinking to the current levels of 3,815 in February of 2016[3], reflecting the strain in which businesses are operating in the tough economic environment. There has been unprecedented levels of profit warnings issued by listed companies, with 12 reported in 2015.

It is however not all doom and gloom. According to a 2015 report by PwC, *Into Africa: The continent's Cities of Opportunity,* Nairobi has been identified as the most attractive destination for foreign direct investment, followed by Accra, with Lagos and Johannesburg joint third. Despite the harsh economic environment, there are tremendous gains being made in the speed at which Kenya is investing and improving its infrastructure and business environment. Investments in the Standard Gauge Railway, road network, electricity generation and distribution as well as telecommunication connectivity are all helping to reduce the cost of doing business across the country.

With all the projects and investments and flow of money into the country, coupled with an economy feeling the heat from fast expansion that is affecting macroeconomic factors, the environment creates opportunities for perpetrators of economic crime to thrive in the absence of strong systems and people committed to operating ethically. There has been a focus on *"the fight against corruption",* with bribery and corruption being a topical issue in the country in the recent past. The Government has come under pressure from various quarters to act against the vice. The Kenya Private Sector Alliance (KEPSA) has been at the forefront of pushing for legislation and have shown their support to have the Anti - Bribery bill enacted into law, as the vice affects both public and private organisations. Our proximity to the Horn of Africa where terrorist group Al Shabaab has been posing a threat to the country's security has necessitated more stringent Anti-money laundering and Counter-Terrorism Financing measures which in turn increase organisations' costs of compliance.

It is in the backdrop of all this that the 2016 Global Economic Crime Survey was conducted and the results reflect the current situation in the country and captures the moods and perceptions of individuals and organisations in Kenya. 61% of the respondents to the survey have indicated having experienced economic crime, placing Kenya among the top most affected countries amongst the 115 countries that participated in the survey. Asset misappropriation, bribery and corruption and procurement fraud were some of the most prevalent forms of economic crimes reported, and cybercrime is increasingly becoming a threat to organisations trying to adapt to the new digital world.

We would like to thank all those who participated in the survey and provided us with their views to enable us compile this report, which we hope would be useful in giving an insight into economic crime trends in the country and assist in combating the vice.

1) Source: The Central Bank of Kenya
2) The Kenya Bureau of Statistics Economic survey of 2015
3) Source: The Kenya Bureau of Statistics

Introduction

We are pleased to present our eighth biennial Global Economic Crime Survey and fourth biennial Kenya report.

With more than 6,000 responses from senior executives in 115 countries, this is the most comprehensive survey of economic crime available to businesses globally, in Africa and in Kenya. It includes 99 respondents from Kenya, which represented about 15% percent of the African respondents.

This summary report, centred on the results for Kenya, seeks to understand and explore trends in economic crimes—including giving you a glimpse of the view amongst Kenyan organisations into the various types of fraud they are exposed to, the attitudes of the organisations towards dealing with these frauds, and the views on how organisations can put in place structures to minimise the incidences.

In this report, the responses from Kenyan participants are also compared with those for the rest of Africa and globally. We also draw a comparison with the results from our 2014 survey to assess what has changed in the two years.

The 99 Kenyan responses from our 2016 survey came from senior representatives of large, medium and small organisations. Of these, 28% are listed companies, 47% are private companies and 14% are government/public sector organisations. Consequently the survey provides a useful indicator for evaluating economic crime and trends for Kenya and comparing it with both regional and global trends as well as the development of fraud trends over the last two years.

Of the different types of economic crimes, incidences of asset misappropriation continue to be the most prevalent both globally and in Kenya. The reported incidences of asset misappropriation were 64% globally and 72% in Kenya. Bribery and corruption was the second most prevalent form of economic crime in Kenya.

Whereas the global average was 24%, Kenya reported 47% incidence of bribery and corruption, the third highest incidence globally. The third most prevalent incident of economic crime as reported in Kenya was Procurement fraud with 37% of the respondents having experienced procurement fraud in the last two years, against a global average of 23%. Other insights and comparisons are detailed in this report as well as in the global report at **www.pwc.com/crimesurvey**

Cybercrime continues to be a growing concern to various organisations both globally and in Kenya. As systems continue to be more complex and connected, the threats of cybercrime increase, and we will explore the effects on organisations and how they are effectively dealing with the digitised threat.

Our findings indicate that 1 in 10 economic crimes are discovered by accident

Our survey this year is focussed on three core areas which resonates with what has been expressed globally as areas of concern, i.e. ethics and compliance programmes in response to the increasing concerns on bribery and corruption incidences as well as negative perceptions of how the problem is being dealt with, Anti-money laundering and Cybercrime. It explores the common themes in the various types of economic crime and the measures put in place by organisations to manage and mitigate these risk areas associated with economic crimes.

The global theme, which is also common from a Kenyan point of view is Opportunity, both in terms of the enablers of economic crime incidences and 0f greatest import to organisations, how they can counter the economic crime trends through continuous and proactive measures.

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

Top 3 most commonly reported types of economic crime in 2016

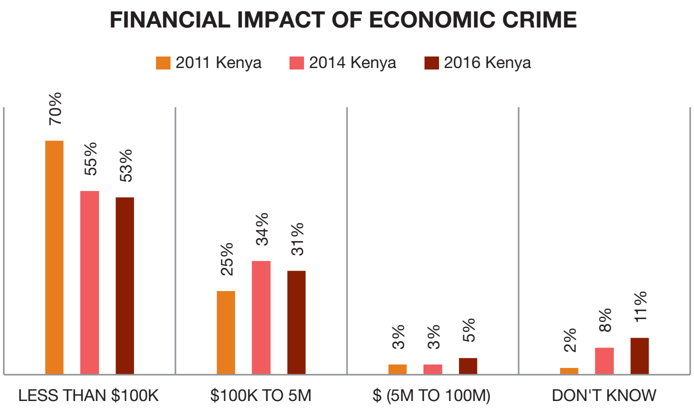
Economic crime in Kenya

Cost of economic crime

The survey reveals an increase in the level of economic crime from the last survey in 2014 with an incidence level of 61% as compared to 52% in 2014, which is 25% above the global average. This placed Kenya joint third with Zambia in 2016 in terms of reported incidences of economic crime from the countries polled. This increase could indicate that the measures implemented to prevent fraud may not be sufficient or effective thereby posing a threat to fundamental business processes.

Interestingly, the cost of economic crime does not appear to be rising significantly. This survey revealed that 58% of respondents in Kenya reported that the cost of economic crime suffered was less than USD100k compared to 55% in 2014. This survey did however reveal that there was a percentage increase of 6% i.e. from 34% to 40%, reported in the higher cost bracket i.e. USD100k to USD5m.

Despite the reported rising level of economic crime suffered, it appears that these crimes are having a lower cost impact as compared to the past. However, the frequency of these low cost incidences of economic crimes are on the increase.



Economic crime does however seem to have a significant impact on reputation/brand strength, employee morale and business relations among most organisations in Kenya. It however appears that economic crime does not have a significant impact on share price.

Types of Economic Crime

The survey revealed the three main types of economic crime committed within organisations in Kenya are asset misappropriation (72%), bribery and corruption (47%) and procurement fraud (37%). This is also true among Africa and global respondents.

Type of Economic Crime	Likelihood of Occurrence		
	Kenya	Africa	Global
Asset misappropriation	72%	69%	64%
Accounting Fraud	33%	27%	18%
Bribery and Corruption	47%	35%	24%
Cybercrime	27%	28%	32%
Intellectual Property Infringement	5%	6%	7%
Money Laundering	5%	12%	11%
Tax Fraud	7%	7%	6%
Insider Dealing	7%	5%	7%
Procurement Fraud	37%	34%	23%
Mortgage Fraud	7%	5%	6%
Competition Law/ Anti-Trust Law infringement		1%	4%
Espionage	3%	1%	2%
Human Resources fraud (recruitment and/or payroll fraud)	18%	20%	12%
Other	8%	12%	11%

Asset Misappropriation

Asset misappropriation is defined as the theft or embezzlement of company assets by directors, other fiduciaries or employees. What is more intriguing is that 68% of respondents are concerned that they will experience asset misappropriation in the next 24 months. This continues to remain the most prevalent and most frequently reported form of economic crime in organisations in Kenya, perhaps because it is regarded as one of the easiest forms of economic crimes to detect.

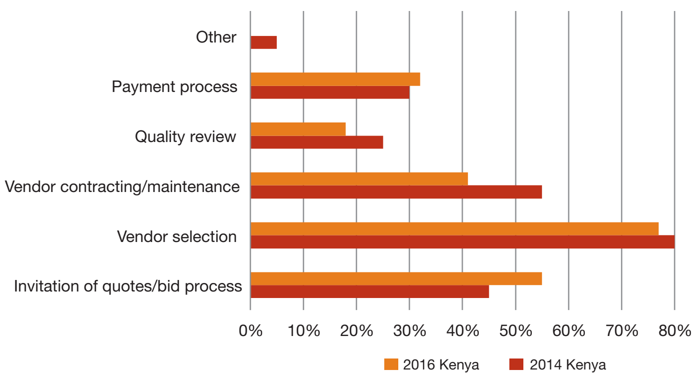
The high incidence indicates that preventative measures such as systems and controls need to be reviewed and new methods of control within organisations introduced as this form of economic crime still poses a high risk among Kenya, Africa and global respondents. The fact that asset misappropriation encompasses a diverse range of economic crimes and fraud, may however result in organisations encountering difficulties in implementing adequate countermeasures.

Procurement Fraud

The 2014 survey reported that 31% of respondents in Kenya experienced procurement fraud. The 2016 survey reveals that this form of economic crime poses an increasing threat to organisations as respondents in Kenya reported incidences of procurement fraud at 37%.

A further analysis of procurement fraud occurrences indicates that 77% of the respondents cited vendor selection process as being most vulnerable to this form of economic crime. This has however reduced compared to the 80% cited by respondents in Kenya in the 2014 survey. The drop is marginal and the incidence level remains high. It is clear that a lot still needs to be done.

PROCUREMENT FRAUD OCCURENCE



Bribery and Corruption

The survey reveals that bribery and corruption is on an increase. According to the Kenyan respondents to the 2012 and 2014 surveys, this form of economic crime accounted for 23% and 27% of the respondents respectively. Respondents to this survey reported bribery and corruption at 47%. This increase is concerning as bribery and corruption poses a significant threat to the growth of the economy and to fair market competition.

It is even more concerning to note that respondents to this survey in Kenya reported that there is a 61% likelihood of their organisations experiencing bribery and corruption in the next twenty four months, and only 46% believe that top level management perceive bribery as an illegitimate practice. This indicates that the mind-set of individuals within the organisations needs to be changed. It is important to also set the right key at the top, as this will greatly influence how individuals within the organisation perceive involvement in bribery and corruption practices.

Countermeasures of economic crimes should aim at addressing transparency and restriction of use of proceeds obtained from these crimes.

The incidences of bribery and corruption are usually in tandem with procurement related frauds. Measures that need to be put in place by organisations to mitigate these economic crimes should be aimed at addressing transparency in the procurement processes and restricting the use of proceeds of these crimes through strict anti-money laundering compliance measures.

Although not linked to this survey, the Kenyan Government seems to recognise that bribery and corruption is a serious issue which needs to be immediately addressed and resolved. Corruption was one of the key issues discussed during President Obama's visit to Kenya in 2015, which resulted in

the Kenyan government signing an agreement with the US to introduce new anti-graft measures. The 29 point deal states, inter alia, that Kenya will step up in investigating corruption cases with increased assistance and advice to Kenya anti-corruption agencies from the US on relevant legislations, and international commitments made by Kenya to joining the Egmont Group of Financial Intelligence Units and the Extractive Industries Transparency Initiative .

These initiatives indicate that Kenya has spear headed its fight against corruption in the correct direction. It is also encouraging to note that the Kenya Leadership and Integrity Forum in Nairobi organised a workshop bringing together the public sector and non- state stakeholders who validated the draft Kenya Integrity Plan for 2015-2019. This plan is structured to provide an understanding for the design and implementation of anti-corruption initiatives by stakeholders .

In view of combatting corruption, towards the year ending 2015, the Government also announced the introduction of new measures to secure ethical business conduct as well as the implementation of new legislations and the strengthening of the legal framework for fighting this form of economic crime. As per these new measures, every organisation in Kenya from 2015 henceforth seeking to conduct business with the government both at a county and national level, will be required to sign an approved Business Code of Ethics domiciled in the Procurement Oversight Authority.

Businesses that fail to comply with this Code will be disqualified from doing business with the government for a period of five years and this information will be made available to the public . This strategy of naming and shaming should prove to be an effective way of discouraging those tempted to engage in corrupt practices.

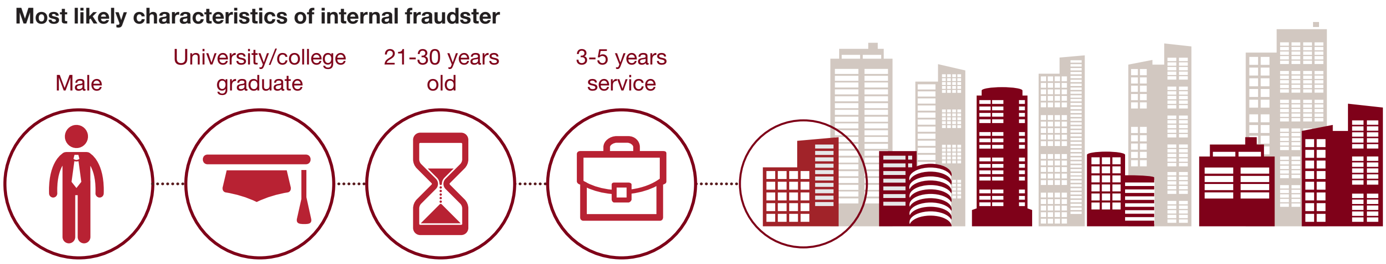
As it is recognised that this form of economic crime is driven by greed, a change of mind-set is necessary. To address this, the President announced that he had directed the Ministry of Education, Science and Technology and related bodies to ensure that values, ethics and integrity awareness is mainstreamed into both the public and private education curriculum with a view of these being examinable. The Government announced that it would also be introducing a compulsory ethics and integrity training programme across all levels of the public service .

Another bid to curb corruption and improve transparency in the Kenyan public procurement system involves the Government introducing the electronic procurement and payment system which was launched in August 2015. These systems were launched with a view to eliminating middlemen and corruption in the government procurement processes .

The private sector has also recognised the threat posed by this particular economic crime and is also supporting the government in pushing for the enactment of laws and controls to counter the increased threat of bribery and corruption. Separately, the private sector is spearheading a national values campaign under the banner “Mkenya Daima”.

The Chairman of the Kenya Private Sector Alliance demonstrated commitment towards fighting corruption in stating that the campaign will paint corruption as being shameful and dishonourable as is those who engage in corrupt practices. In addition, the private sector provided to the Government a proposed anti-bribery bill . This bill is intended to focus on the supply side of corruption, on those who give bribes or induce government officials. Among other measures, it will penalise the failure by commercial organisations to prevent bribery[10].

4) Kenya’s Renewed Commitment to Fight Corruption Needs the Private Sector *http://www.cipe.org/blog/2015/09/14/kenyas-renewed-commitment-to-fight-corruption-needs-the-private-sector/*
5) Five year integrity plan gets stakeholders nod *http://www.eacc.go.ke/whatsnew.asp?id=671*
6) The Presidency – The Official Website of the President – Statement made by the President on 23 November 2015 *http://www.president.go.ke/2015/11/23/statement-by-his-excellency-hon-uhuru-kenyatta-c-g-h-president-and-commander-in-chief-of-the-defence-forces-of-the-republic-of-kenya-on-a-national-call-to-action-against-corruption-state-house/*
7) The Presidency – The Official Website of the President – Statement made by the President on 23 November 2015 *http://www.president.go.ke/2015/11/23/statement-by-his-excellency-hon-uhuru-kenyatta-c-g-h-president-and-commander-in-chief-of-the-defence-forces-of-the-republic-of-kenya-on-a-national-call-to-action-against-corruption-state-house/*
8) State corruption slowing business growth, Kepsa warns *http://www.nation.co.ke/business/Pervasive-corruption-hurting-business/-/996/2921966/-/41irot/-/index.html*
9) KEPSA *http://www.kepsa.or.ke/2015/12/04/kepsa-meets-with-county-executives-to-reflect-on-competitiveness-in-the-counties/*
10) The Presidency – The Official Website of the President – Statement made by the President on 23 November 2015 *http://www.president.go.ke/2015/11/23/statement-by-his-excellency-hon-uhuru-kenyatta-c-g-h-president-and-commander-in-chief-of-the-defence-forces-of-the-republic-of-kenya-on-a-national-call-to-action-against-corruption-state-house/*



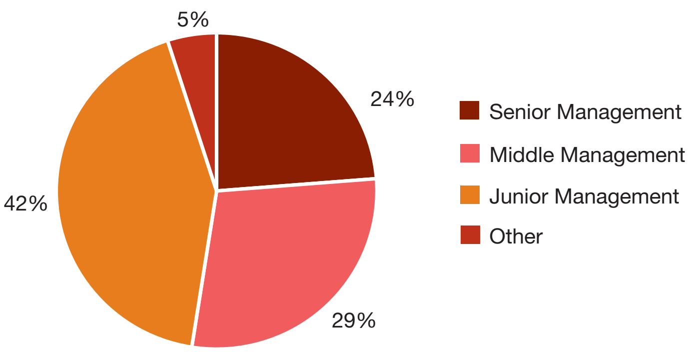
Who is committing the fraud and how do organisations deal with the perpetrators?

Internal Fraudster

Similar to previous survey trends, most economic crimes continue to be committed by internal actors. According to this survey and in the case of respondents who reported having suffered economic crime, internal fraudsters were responsible for 70% of the cases reported by Kenyan organisations. The Global and Africa respondents total for internal fraudsters was 46% and 53% respectively.

Out of the internal fraud perpetrators, and what is a new trend amongst Kenyan respondents, the survey indicated that it is junior management that was responsible for the largest percentage of the economic crimes committed by staff.

LEVEL OF INTERNAL FRAUDSTER

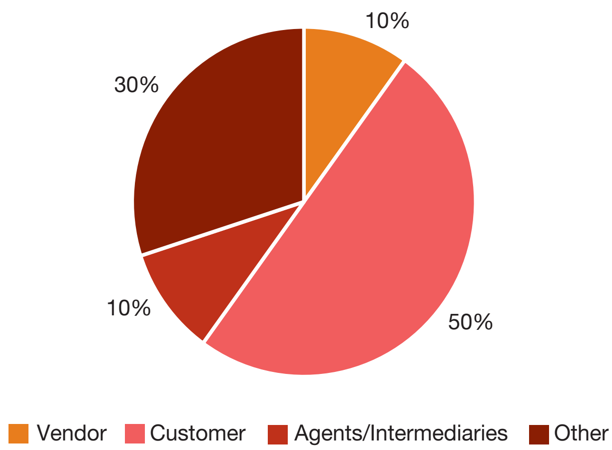


When dealing with internal fraudsters, this survey revealed that most Kenyan organisations dismissed the perpetrator (74%) which is a similar course of action followed globally (76%) and in Africa (78%). The survey revealed that more than half of the organisations in Kenya also contacted law enforcement (55%). This suggests that organisation are now adopting serious courses of action to deal with economic crimes so as to help prevent future incidents of fraud occurring.

External Fraudsters

Among the external fraudsters, customers lead the pack of external fraudsters in Kenya with 50% of respondents identifying this group as the main perpetrator. Agents/ Intermediaries and Vendors represent 10% each. With customers being the primary external fraudster, this would suggest that business models need to be reviewed and processes implemented to prevent organisations from becoming prey to fraudulent activity.

IDENTITY OF EXTERNAL FRAUDSTERS?



This survey reveals that when dealing with external fraudsters, the most popular action taken is to inform law enforcement as reported by 56% of respondents in Kenya. This approach taken by Kenya mirrors the global and Africa response at 53% and 68% respectively. The second preferred course of action taken by Kenyan organisations in dealing

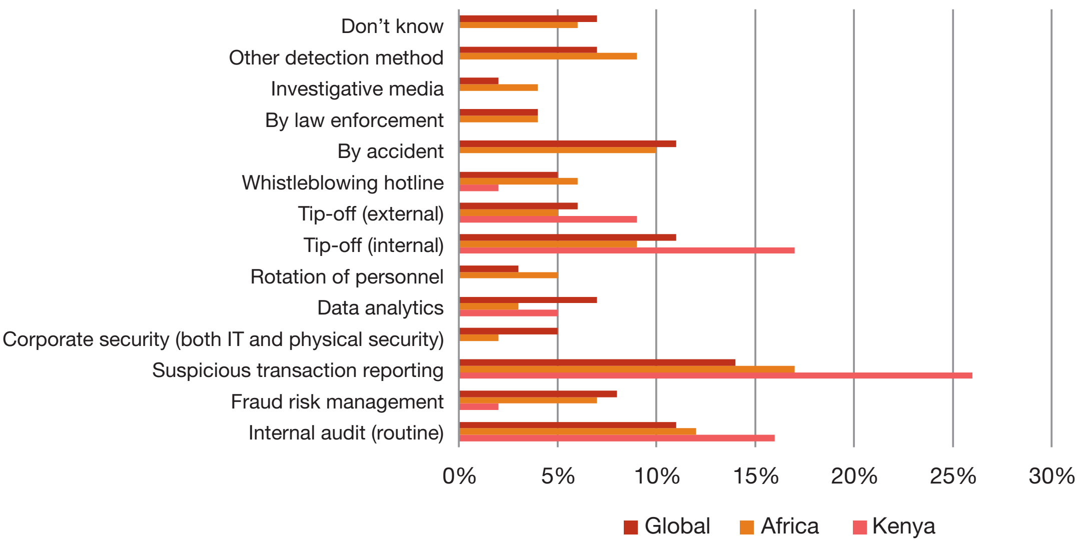
with external fraudsters is to notify the relevant regulatory authorities (44%). Civil action and cessation appear to be the least preferred action taken by Kenya with only 33% of respondents resorting to each of these actions. This may be as a result of the long court processes as far as civil proceedings are concerned.

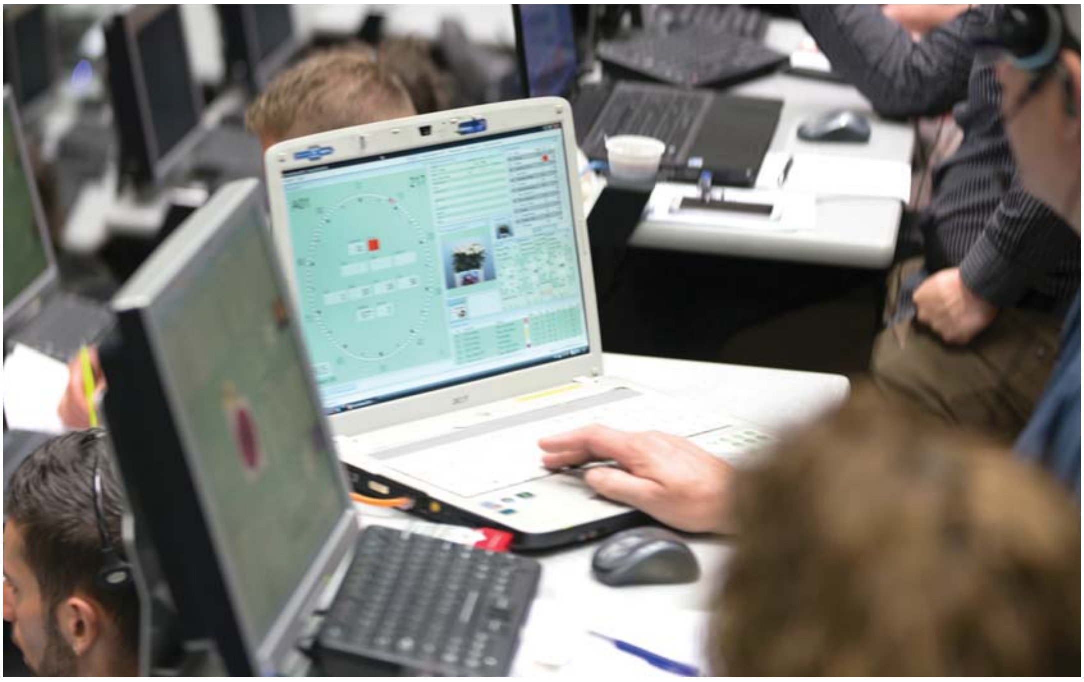
What is particularly worrying in the survey is the low levels of confidence in local law enforcement's ability to investigate and prosecute economic crimes. Respondents in Kenya and South Africa were the least confident in the local law enforcement's ability to investigate and prosecute economic crimes with Kenyan respondents the most pessimistic globally at 79%. This against a global average of 44%.

Detecting economic crime

How prepared is your organisation? The methods of fraud detection vary. This survey reported that the most common way for organisations in Kenya to detect economic crime in the past twenty four months has been through suspicious transaction reporting (26%). This is also true among Africa respondents (17%). Detecting economic crime via suspicious transaction reporting implies that individuals within organisations have an understanding of economic crime and what could potentially constitute economic crime. Only 2% of the respondents within Kenya stated that economic crime was detected via fraud risk management.

FRAUD DETECTION METHODS

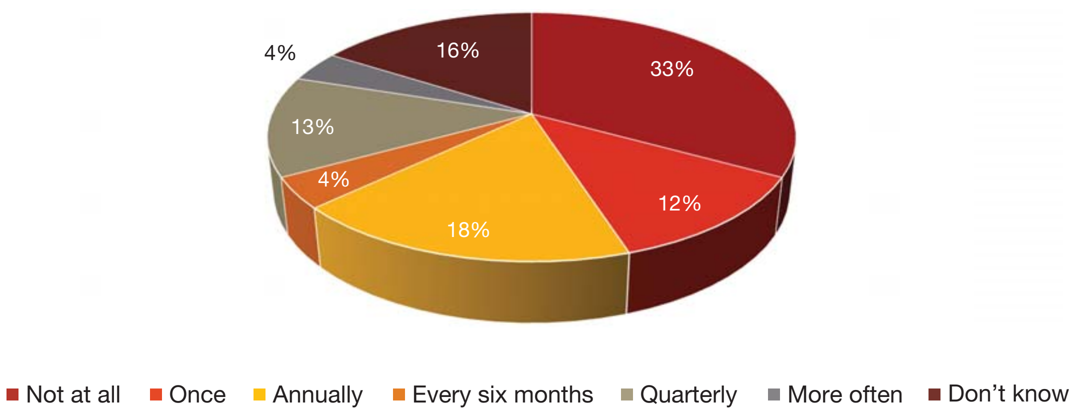




As indicated above, a small percentage of respondents in Kenya (2%) undertake fraud risk management as a way of detecting fraud, a trend replicated globally (8%) and in Africa (7%) which may explain the infrequency of detection through fraud risk assessments. This is the implementation of continuous assessments of the organisation's preparedness in dealing with fraud. Fraud risk assessments help keep the organisation to remain on the lookout for new threats and risks of fraud, as fraud schemes are always evolving.

The majority of respondents in Kenya - a total of 33%, reported that in the last twenty four months there was no fraud risk assessment conducted. As fraud risk assessments are considered to be an effective and efficient way of detecting and preventing economic crime, it is essential for organisations in Kenya to focus on introducing such assessments to help better protect themselves from economic crime.

FREQUENCY OF FRAUD RISK ASSESSMENTS



Special focus on cybercrime and money laundering in Kenya

Cybercrime

61% Of respondents have had an increase in their awareness and perception of the exposure of their organisations to cybercrime risks. Do you keep pace with the changing digital landscape and the evolving digital frauds that your organisation is exposed to?

33% A third of the respondents have been affected by cybercrime in the last 24 months. How is your organisation coping with the increase in the cybercrime threats and incidences?

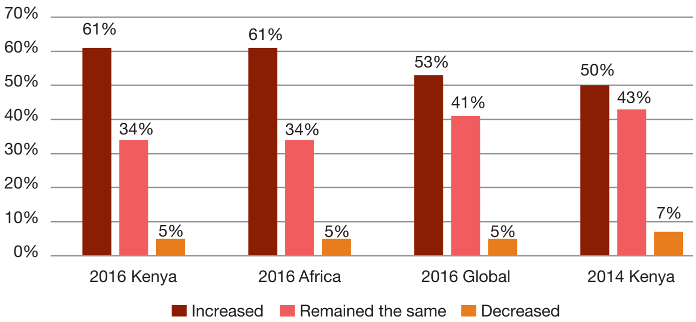
32% Of respondents suffered significant financial impact from the incidences of cybercrime they encountered. What is the cost of cybercrime to your organisation? Is it worth investing in counter systems and measures?'

Cybercrime includes distributing viruses, phishing and pharming, stealing personal information and illegally downloading files.

Cybercrime, mostly associated with computer related crime, is a form of economic crime committed using digital devices and the internet. Given that many tablets and smart phones nowadays have computer like capabilities, the definition of cybercrime can be extended to such devices.

This is extremely relevant in the Kenyan context given that a large proportion of the Kenyan population has access to computing facilities and the internet. As was explained in the previous survey, cybercrime includes distributing viruses, phishing and pharming, stealing personal information and illegally downloading files.

CHANGE OF PERCEPTION ON RISK OF CYBERCRIME



The perception of risk of cybercrime is increasing. This could be because the advancement of technology in business services, combined with a rapid growth in data connectivity and social media has altered business landscapes[11]. This year, 61% of the respondents said that their perception of cybercrime risk at their organisation has increased, up from 50% in 2014.

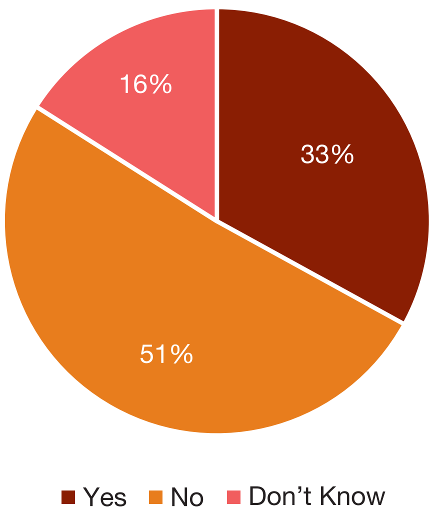
11) Global Economic Crime Survey 2014 *http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/cybercrime.html*

Though the perception of the risk cybercrime poses to organisations is increasing, only a small percentage of organisations have an incident response plan to deal with cyber-attacks. Only 30% of respondents in Kenya reported that their organisation has an incident response plan which is implemented and fully in operation.

A total of 26% of the respondents reported that their organisation did not have an incident response plan in force, but were in the process of assessing the feasibility of implementing such a plan. A further 14% of respondents reported that there was no incident response plan implemented and there were no intentions of implementing such a plan. These results are of concern given the rate at which cybercrime is increasing and as was provided in the Global Economic Crime Survey 2014, organisations do not realise that they are a target of cybercrime until long after the damage is done.

About 27% of organisations in Kenya have reported having been victim to cybercrime as compared to the global reported incidence levels of 32%. Though below the global average, the incidences have been slowly growing over the years. In 2014, 22% of organisations reported having experienced cybercrime. Half of the respondents in Kenya reported that their organisations were not affected by cybercrime.

% OF ORGANISATIONS BEING AFFECTED BY CYBERCRIME



11%

Of respondents who reported that their organisations did not have a first responder and this was only because they felt that one was not needed.

Fortunately, a majority of organisations in Kenya have identified first responders who are able to mobilise within a short period of time should a technology breach occur. A total of 32% of respondents said that they had internal personnel who had undergone first responder training to act as and when the need arises.

Only 11% of respondents reported that their organisations did not have a first responder and this was only because they felt that one was not needed. When asked which types of specialists the organisations first responder team included, 73% of the respondents stated IT Security. As cybercrime can potentially have an adverse impact on organisations, these results provide reassurance in terms of organisations being able to proactively react in the event of a cybercrime incident.

An area of concern however in the fight against cybercrime is the lack of confidence in local law enforcement agencies to have the required resources and skills to investigate cybercrime, hacking incidents and malware related frauds (73% of the Kenyan respondents indicated a lack of confidence). This therefore suggests that cybercrime fraudsters are able to easily launch cyber-attacks and even worse, get away with it.

There are a few possible explanations for the low confidence numbers. Cybercrime evolves at a rapid rate, and the resources and degree of sophistication needed to keep up is often beyond most law enforcement agencies. The lack of borders in the cyber-world within which attacks originate and the complexity of jurisdictions in which law enforcement agencies can follow up the criminals makes investigations and prosecution even more difficult.

Worth noting in particular is the fact that among the top 10 countries exhibiting low confidence levels in their law enforcement were such developed economies as the United States, the United Kingdom and Luxembourg, thus dispelling the notion that this might be an issue only prevalent in developing or underdeveloped countries.

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

The threat of organisations being affected by cybercrime is increasing and thus, the key question is, what potential measures can an organisation adopt to defend itself against cyber security attacks?

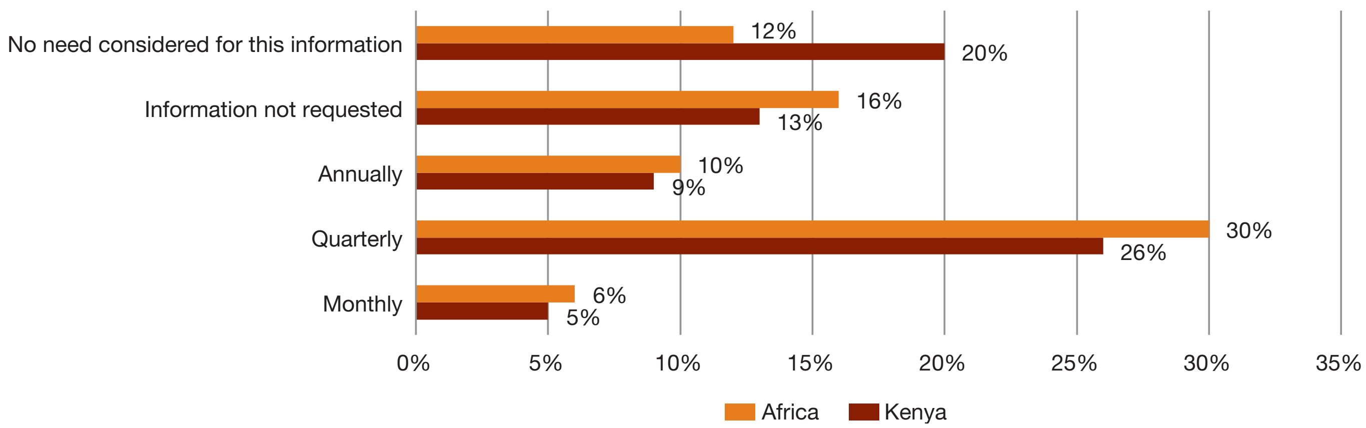
> *Having a good management that keeps abreast of trends is vital as no system is impervious as combatting cybercrime can be compared to a game of cat and mouse[12].*

With this point in mind, this survey has reported disappointing results in terms of how often Board members within organisations in Kenya and Africa request information regarding the organisations' state of readiness to deal with cyber incidents.

- Adopting a risk based framework will allow for companies to efficiently communicate and collaborate on cybersecurity measures, both internally and externally. Implementing a risk based framework will help organisations to better design, monitor and review, and measure goals directed towards improving cybercrime prevention measures. This approach will also ensure that sensitive data is more secure[15]. It is also essential for the Board of Directors to treat cybersecurity as a corporate risk issue rather than simply a risk facing IT alone[16].

- Ensure that organisations have a cyber incident response team as this will enable organisations to systematically respond to cyber threats and incidents. As stated in previous Global Economic Crime Survey Reports, a well-functioning response team will enable organisations to identify potential cyber threats and act upon mitigating the threat in an efficient and effective manner. In addition, the cyber incident response team must frequently review the effectiveness of the preventative measures implemented, including systems and controls. This will mean that the organisation has to adopt a proactive approach to fighting cybercrime rather than a reactive approach.

FREQUENCY OF BOARD MEMBERS REQUESTING INFORMATION AS TO THE ORGANISATIONS ABILITY TO DEAL WITH CYBER INCIDENTS



It is necessary for security executives, senior management and the Board of Directors to play prominent roles so as to prevent organisations from falling victim to cybercrime incidences. According to the Global State of Information Security Survey 2016, it is a pre-requisite for top executives to not only have expertise in security but also in corporate governance, risk management, and overall business objectives[13].

This involvement and commitment will help improve cybersecurity and better align overall risk management and business goals with information security[14]. As has also been mentioned in previous Global Economic Crime Surveys, senior management should also play an active role in ensuring that roles and responsibilities are transparent and clear.

- According to The Global State of Information Security Survey 2016, investing in cloud computing is a sophisticated way of enabling organisations to improve their intelligence gathering and threat modelling. This will help to better protect data and network security.

- Being able to fight cybercrime will require organisations to understand and be aware of the various kinds of cybercrime threats which potentially face the organisation. Organisations must therefore, as has been highlighted in previous Global Economic Crime Survey Reports, educate employees and provide necessary training to equip employees with the skills and knowledge to be able to prevent and manage cybercrime attacks.

12) Respond to cybercrime and data breach - *http://www.pwc.com/us/en/forensic-services/cybercrime.html*
13) The Global State of Information Security Survey 2016 - *http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/key-findings.html*
14) The Global State of Information Security Survey 2016
15) The Global State of Information Security Survey 2016
16) Key findings from the 2015 US State of Cybercrime Survey - *http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf*

Money Laundering

73% Of financial services respondents have carried out money laundering or terrorist financing risk assessments. Is your organisation updating its systems to monitor suspicious flow of funds from questionable sources?

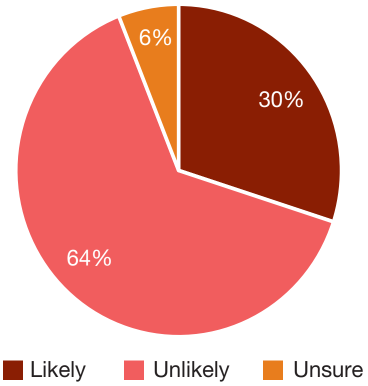
33% The two biggest challenges to effective AML compliance cited by financial industry firms are the technology requirements (33%) and complying with AML requirements from multiple jurisdictions (29%). Are you planning to invest in technology to assist in improving the monitoring of suspicious transactions which is adaptable to a changing risk landscape and increasing regulatory expectations? Are you struggling with differing legal requirements in the countries in which your organisation operates?

51% about half of the non-financial services firms' respondents are monitoring for AML/ CFT-specific red flags for their industry. Are you up to speed on the latest requirements you must meet?

64% of respondents in Kenya reported that it is unlikely that the organisation will experience money laundering in the next twenty four months.

According to the results of this survey, money laundering does not seem to be of major concern. Only 5% of respondents in Kenya reported money laundering as an economic crime experienced in their organisation. It is also positive to note that 64% of respondents in Kenya reported that it is unlikely that the organisation will experience money laundering in the next twenty four months.

LIKELIHOOD OF ORGANISATIONS EXPERIENCING MONEY LAUNDERING IN THE NEXT 24 MONTHS



These results are encouraging as it implies that organisations are meeting compliance standards.

Throughout 2015, regulatory pressures concerning Anti- Money Laundering (AML) continued to rise. There has been an increase in pressure surrounding compliance matters with AML and Know Your Customer ("KYC") requirements. This therefore requires management to focus on ensuring that a robust and appropriate compliance framework is embedded within the organisation.

Bordering the volatile Horn of Africa region where incidences of terrorism and piracy pose a great threat to Kenya, it is increasingly important to monitor the potential integration of proceeds of crime into the Kenyan economy as well as to monitor the raising of finances for terrorist activities. Terrorism financing is also on the radar of governments globally as terrorism has in the last few years spilled over to regions and countries that historically have not been targeted by terrorist organisations.

On AML, multi-national companies that have been found to have flouted AML compliance requirements have been assessed and fined in the hundreds of millions to billion dollars by watchdogs in the US, and other countries are following suit in tightening regulation and enforcement in light of the global threats.

Traditional off-shore jurisdictions in which ill-gotten funds have in the past been funnelled are also coming under closer scrutiny and greater transparency is being demanded from them globally.

AML compliance requirements are also being cascaded to non-banking institutions that are involved in financial transactions including mobile money transfer, insurance and asset management companies. The complexity of regulations will imply greater costs to institutions to comply.

According to new figures from WealthInsights, global spending on AML compliance is set to grow to more than $8 billion by 2017 (a compounded annual growth rate of almost 9%)[17]. Cost sensitivities leave most organisations in a dilemma over increasing compliance spend — notwithstanding the cost of enforcement actions and large-scale penalties resulting from compliance failures.

So what does this mean to organisations and the staff? Where is the opportunity given these developments both in Kenya and globally?

They can stay ahead of the regulatory curve – While the rest of corporate Kenya is rushing to comply and put in place structures to comply with both local and global AML compliance requirements, it would be cost effective and more manageable to your organisation if you stay on top of and preferably ahead of regulatory changes which are continuously being harmonized and standardised.

Learn from other institutions' mistakes – Though Kenya has not had headline making cases of penalties by the regulators, with regulatory changes and stricter monitoring of compliance with AML regulations, your organisation should not wait to set precedence and incur the first fines. The cost of remediation and compliance in all cases is less than the cost of the penalties imposed for non-compliance.

Invest in the right resources to assist in ensuring your company is compliant with the regulatory requirements. This may mean investing in technology and qualified people to assist in this. There is however a global challenge in getting the right talent to fill these positions.

Like all forms of economic crime, there is no text-book method of moving proceeds of crime. With tightening of money laundering control measures, criminals will explore new ways of beating the system, and therefore regular risk assessments are critical. From the survey, it is worth noting that 73% of respondents in the financial services firms conducted AML risk assessments in their organisations.

17) Statistics provided courtesy of WealthInsight

Conclusion

Economic crimes remain an area of risk that keeps most organisations and their management teams on their guard. Kenya as a country with its fast rate of growth and development especially in technology is experiencing an era of increased access to information which makes public most bribery and corruption incidents especially in the public sector.

New threats presented by digital communication and hazy regulation with respect to cybercrime in an increasingly integrated world means organisations have to come up with more innovative ways to deal with these threats.

Investing in systems to combat economic crimes needs to go hand in hand with investing in the people that are entrusted with the assets and systems in these organisations. As has been experienced time and again, the costs of not investing in improving the environment in terms of systems, training the workforce and continuously having in place fraud risk management framework to both deter and deal with fraud and other forms of economic crimes can be far greater than the short term savings obtained in cutting costs and hoping for the best. The statistics may not look encouraging, but there is plenty of room to do something about it.

Finally the “right tone needs to be set at the top”. If leadership and management teams of organisations lead the way in ensuring the organisations are compliant and operate in an ethical manner, and they lead by example in having zero tolerance to these economic crimes, the message will trickle down and incidences of economic crimes are likely to reduce.

Contact us

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

Forensic Services Leader

Muniu Thoithi
Forensics Partner, Eastern Africa

t: +254 (20) 285 5684
e: muniu.thoithi@ke.pwc.com

The PwC Forensic Team

George Weru
Senior Manager, Kenya

t: +254 (20) 285 5360
e: george.weru@ke.pwc.com

John Kamau
Senior Manager, Kenya

t: +254 (20) 285 5065
e: john.kamau@ke.pwc.com

Eric Owino
Manager, Kenya

t: +254 (20) 285 5692
e: eric.owino@ke.pwc.com

Stephen Omuga
Manager, Kenya

t: +254 (20) 285 5392
e: stephen.omuga@ke.pwc.com

Participation statistics

Participation statistics

6,337 completed surveys

Across 115 countries

Surveyed in 17 different languages

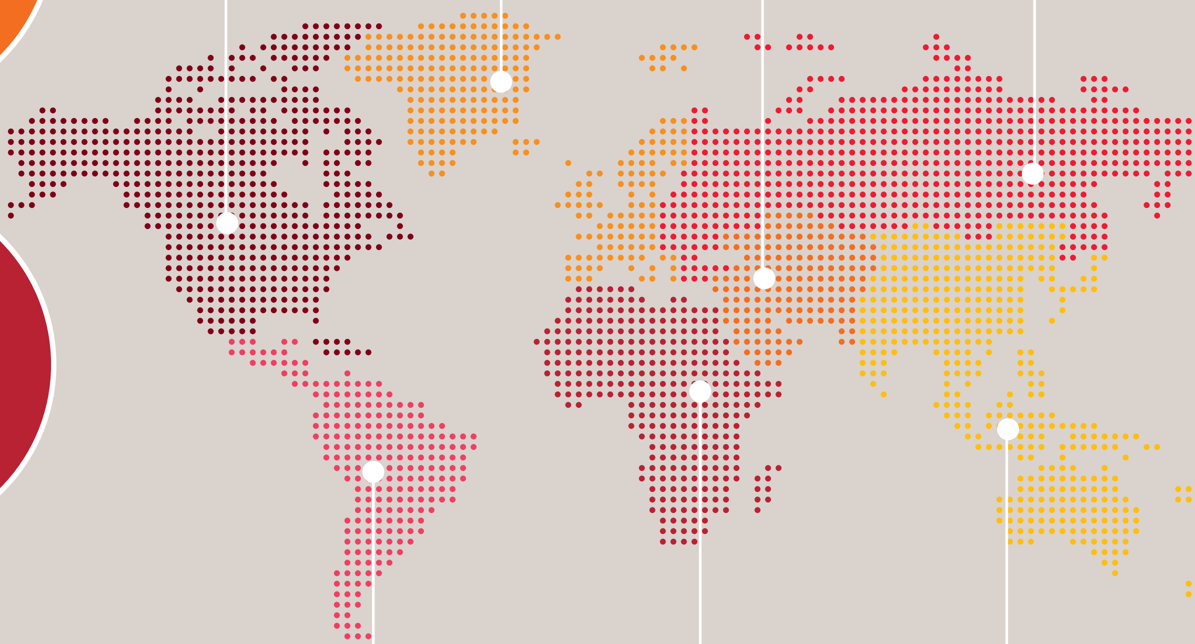
Participation by region

8% North America

22% Western Europe

5% Middle East

17% Eastern Europe



18% Latin America

10% Africa

20% Asia Pacific

Respondents

45%
C-suite

30%
Head of Department or Business unit

70%
of respondents were managing the Finance, Executive Management, Audit, Compliance and Risk Management Functions

54%
of respondents employed by organisations with more than 1,000 employees, with

48%
of these participants having more than 10,000 employees

37%
of the survey population represented Publicly Traded Companies, and

59%
of respondents were from multinational organisations

Industry sectors

35%
Industrial

24%
Financial Services

14%
Consumer

7%
Technology

6%
Professional Services

13%
Other