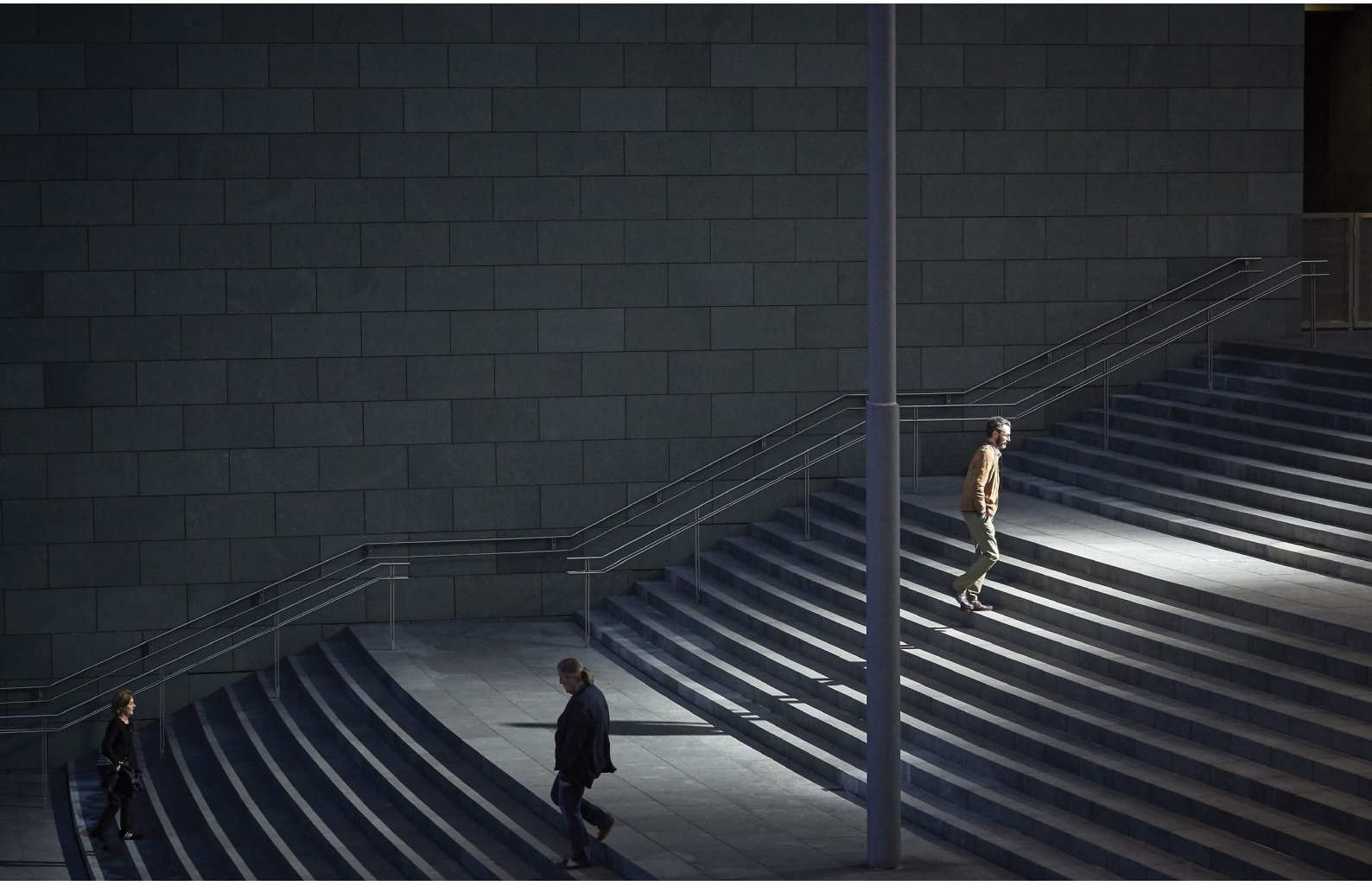
Global Economic Crime and Fraud Survey 2018
6th South African edition
February 2018

The dawn of proactivity: Countering threats from inside and out



pwc

www.pwc.com/fraudsurvey


↓ Prøvesalen

Contents

Leading observations

1 *Rising rates of economic crime continue to disrupt business*

- South African organisations that have experienced economic crime is now at a staggering 77%!
- Companies today face fraud risk from various avenues – internal, external, regulatory and reputational
- Senior management taking front stage as a growing threat from within organisations
- The face of the threat evolves as fraud committed by consumers comes out of the shadows to rank as second most reported economic crime

How will you reassure investors when your tone at the top does not correspond with action from the top?

2 *Detection of economic crime takes on a more proactive stance*

- Organisations taking back control over the detection of economic crime
- Signs of increased spending being committed to combating economic crime and fraud
- Environments within organisations more receptive to trusting internal tip-off processes
- Heightened levels of awareness among the executive suite correspond with increased levels of accountability exercised by the jury of public opinion

Is your organisation following the trend of increased awareness or will you be found wanting?

3

Regulatory risk driving corporate behaviour, but reputation has become key

- Increased levels of regulatory scrutiny and enforcement seen globally
- 71% of respondents expect recent geopolitical regulatory changes to result in changes to enforcement
- Only 37% of respondents have conducted an anti-bribery/ anti-corruption risk assessment
- One in three organisations cite business misconduct as an emerging threat

How will you fare when judged by the jury of public opinion?

4

True cost of economic crime a cause for great concern

- 19% of organisations have had to spend between twice and ten times as much on investigations as the original amount lost to economic crime
- Rightly or wrongly, CEO and board increasingly being held accountable
- Investment in people seen as an effective antidote to fraud

How do you change your policies from words on paper to an indication of your organisational culture?

Foreword

Trevor White
Partner, Forensic Services
PwC South Africa
Global Economic Crime and Fraud Survey Leader

Economic crime continues to disrupt business, with this year's results showing a steep incline in reported instances of economic crime in South Africa – once again we have the dubious honour of having the highest levels in the world, at a staggering 77%!

The global results were equally dismal, revealing the highest level of reported fraud and economic crime since this thought leadership publication was launched in 2001.

We believe that these jumps in reported crime are being driven by a heightened state of fraud awareness by respondents, and in this lies the silver lining. After a long malaise, organisations, driven perhaps by a vigilant jury of public opinion, have become wary of not only the afflictions that may affect them but also the negative impact of being seen to be doing nothing. While the tone at the top is still seen as important, visible action from the top has become vital to survival.

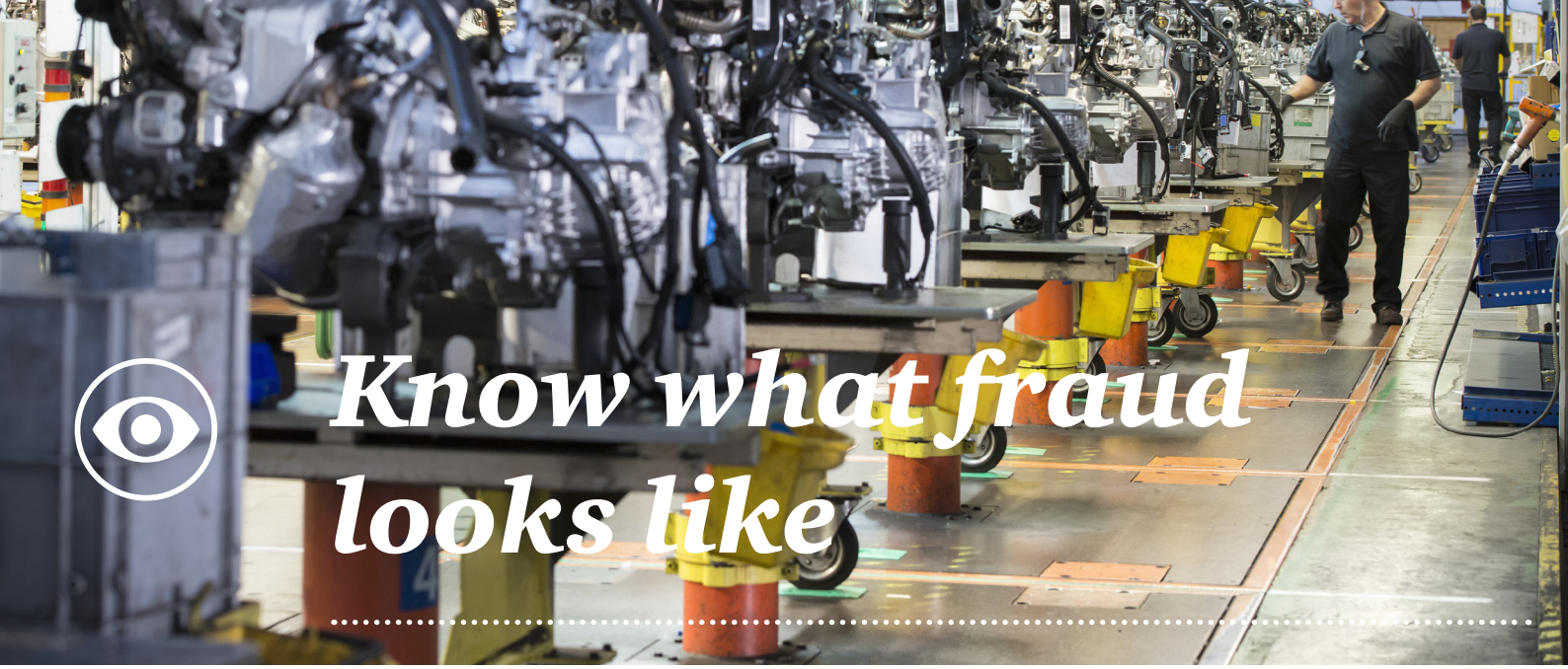
We have witnessed paradigm shifts in the manner and style that businesses are being run:

- Accountability for fraud and economic crime has moved into the executive suite, with the C-suite increasingly taking responsibility, and the fall, when economic crime and fraud occur.
- Organisations are beginning to shed their denial complex regarding the many blind spots they have in identifying fraud and are learning how to address them.
- Changes to the legal and geopolitical landscapes are driving greater awareness and visibility regarding how and why fraud occurs.

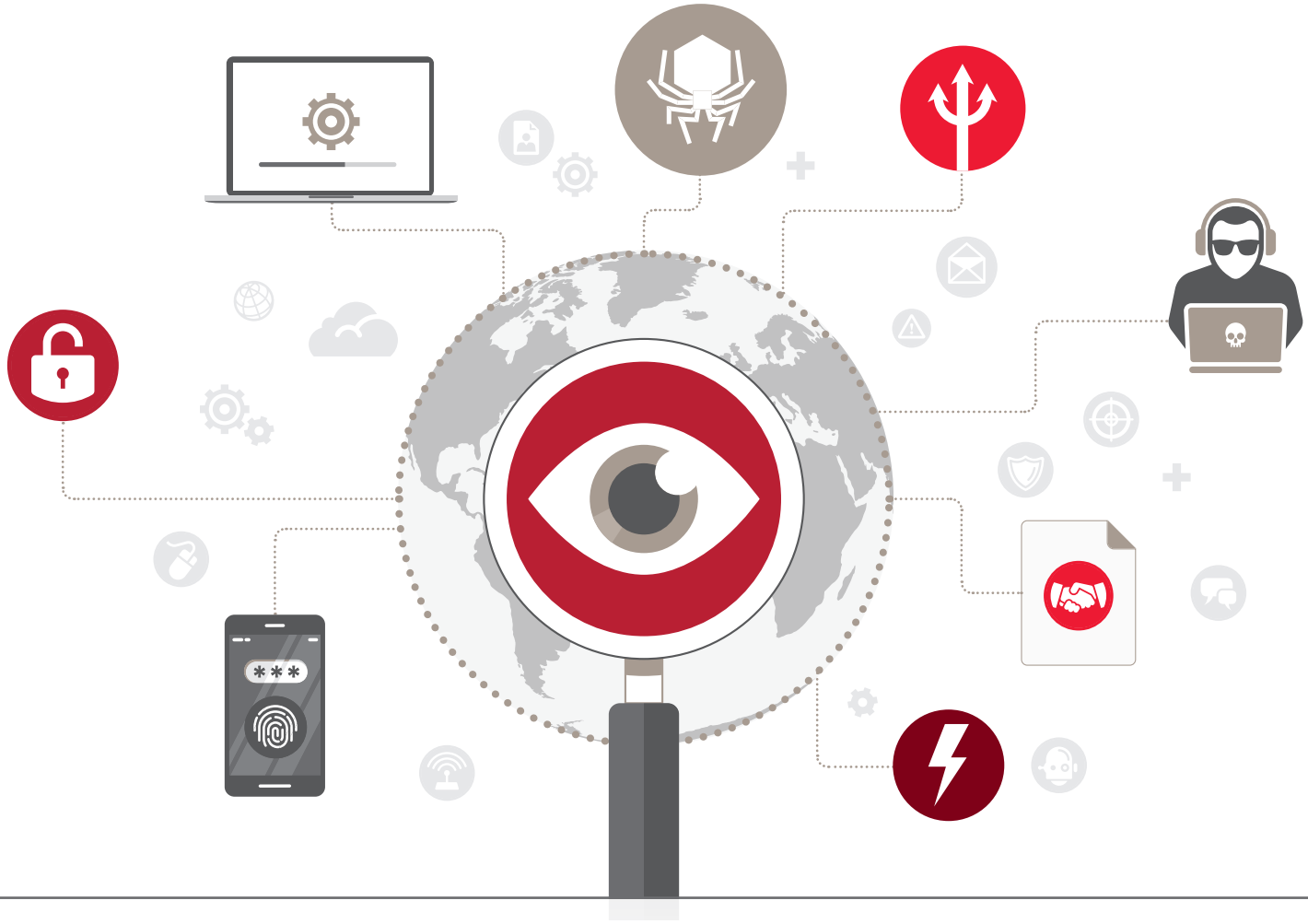
This greater awareness, combined with heightened scrutiny by, and accompanying pressure from, the public for organisations to 'behave', has created an opportunity for active responses to be implemented. The need today is for pre-emptive strikes against a known, yet elusive enemy, both domestic and foreign.

Fraud risk has been seen to emerge with as much prominence from within organisations as it does from outside. We are always on the lookout for the enemies at the gate, but what about the enemies already inside? And not just anyone: often, it's the ones holding the keys to the kingdom... The conventional arsenal is no longer going to cut it, and a more holistic and collaborative view of your organisation is necessary.

We hope that this report will help shed light on those areas that organisations have stopped seeing and will prompt them to take a closer look and identify the gaps that exist. Our wish is for awareness to be further heightened and for a new dawn to break – the dawn of proactivity in the fight against economic crime.



Know what fraud looks like



How well do South Africans know the fraud that affects them?

In this, our sixth instalment of the Global Economic Crime and Fraud Survey, we introduced a question asking respondents to give an indication of their level of insight into fraud and economic crime in their organisation. 70% of South African respondents indicated high or extensive knowledge, while the global response was 60%. This shows that while South Africa emerged with the highest reported rate of economic crime, it is apparent that we have a greater level of awareness of the issues and challenges we face, in comparison to the rest of the world.

It is arguably far better to know and have visibility of issues than to wallow in ignorance, oblivious of the enemy at the gate – especially one that is as formidable and damaging as economic crime and fraud. So now that we know we have a problem, how aware are we of the issues we face?

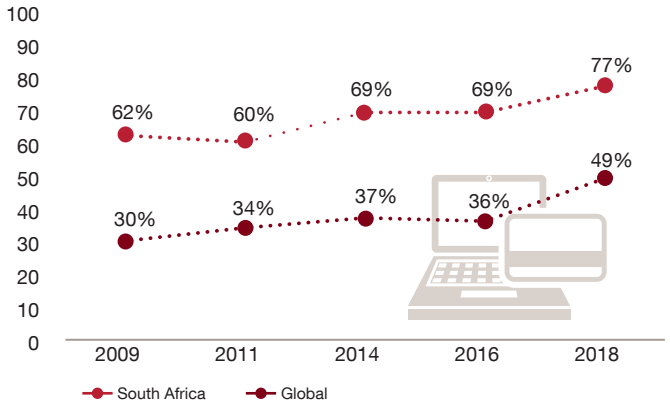
Reported rate of economic crime

This much is certain: we witnessed an upsurge in the number of respondents that indicated that they had been affected by economic crime over the preceding two years. At 77%, South Africa's rate of reported economic crime remains significantly higher than the global average rate of 49%. However, this year saw an unprecedented growth in the global trend, with a 36% period-on-period increase since 2016.

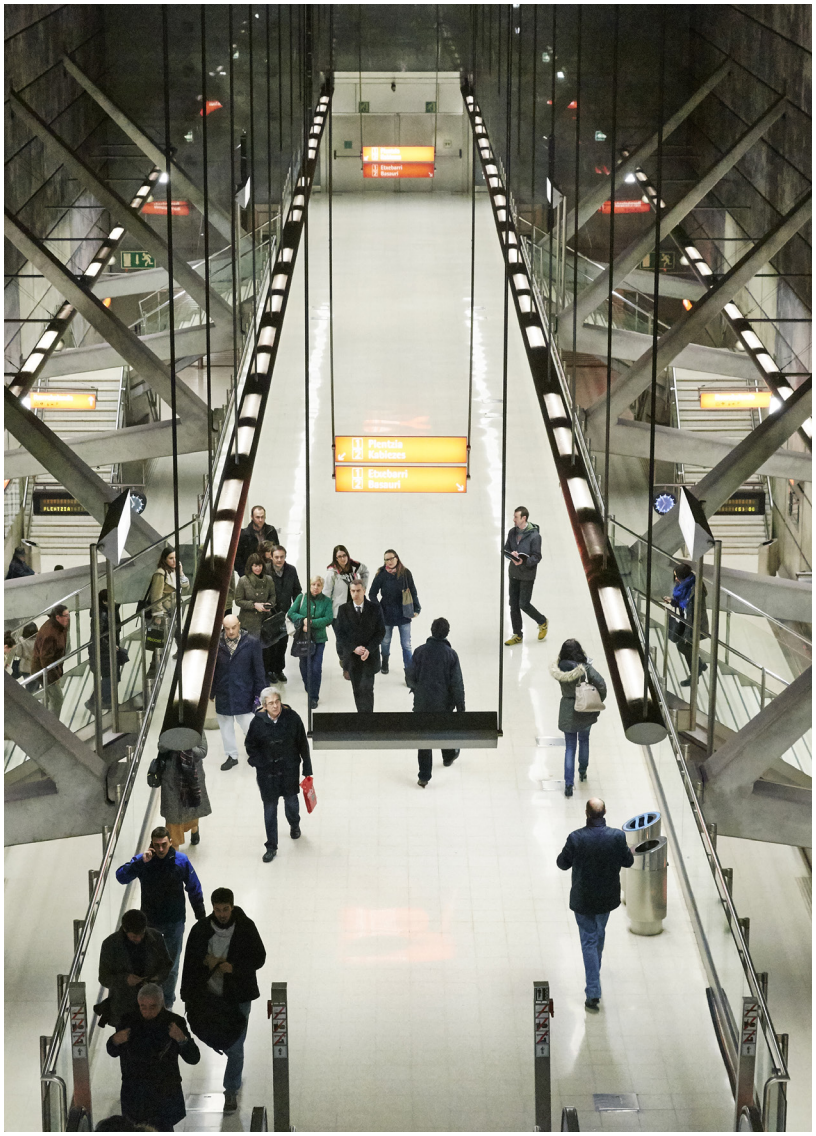
Economic crime in South Africa is now at the highest level over the past decade. Alarmingly, we still found that 6% of executives in South Africa (Africa 5% and Global 7%) simply did not know whether their respective organisations were being affected by economic crime or not.

Companies today face a perfect storm of fraud risk – internal, external, regulatory and reputational

Figure 01: The reported rate of economic crime

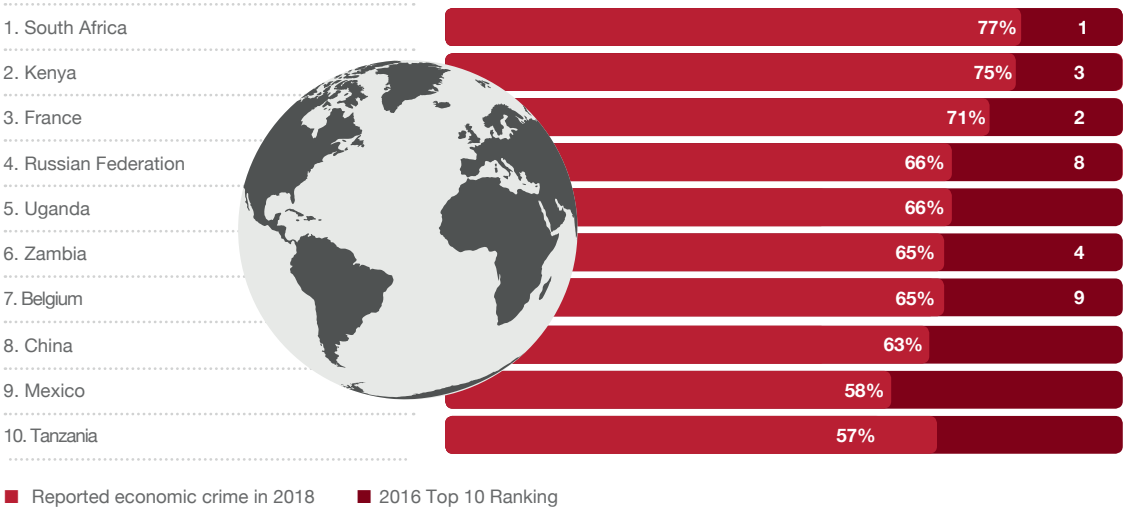


Q. Has your organisation experienced any fraud and/or economic crime within the last 24 months?



South Africa has again reported the highest percentage of economic crime in the world, with Kenya second and France third. With half of the top ten countries who reported economic crime coming from Africa, the situation at home is more than dire.

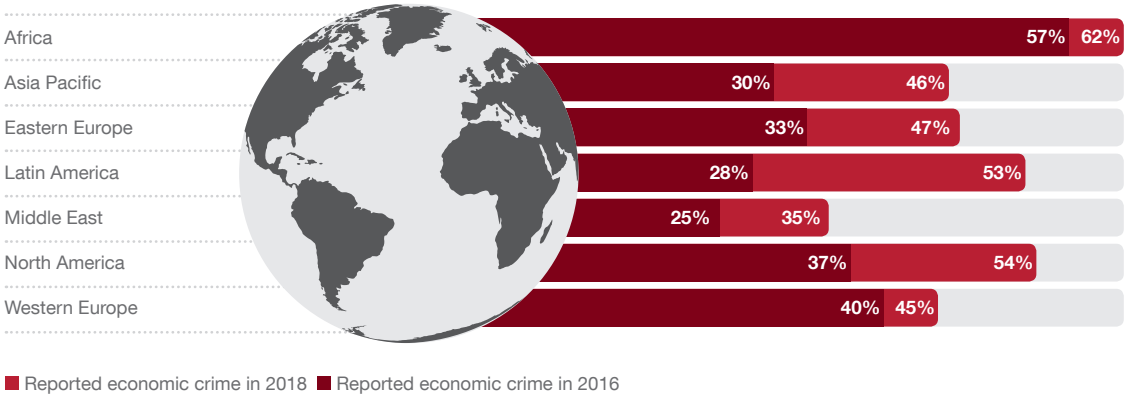
Figure 02: Top 10 countries reporting most economic crime



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

While the overall rate of economic crime reported was indeed the highest for South Africa, the period-on-period rate of increase for South Africa and Africa as a whole was below that of our American, Asian and European counterparts. From a regional perspective, the biggest increase in experiences of economic crime occurred in Latin America, where there was a 25% increase since 2016 to 53% in respondents who indicated that they had experienced economic crime. The United States was a close second with a 17% increase over 2016 to 54% of respondents, while Asia Pacific and Eastern Europe experienced increases of 16% and 14%, respectively.

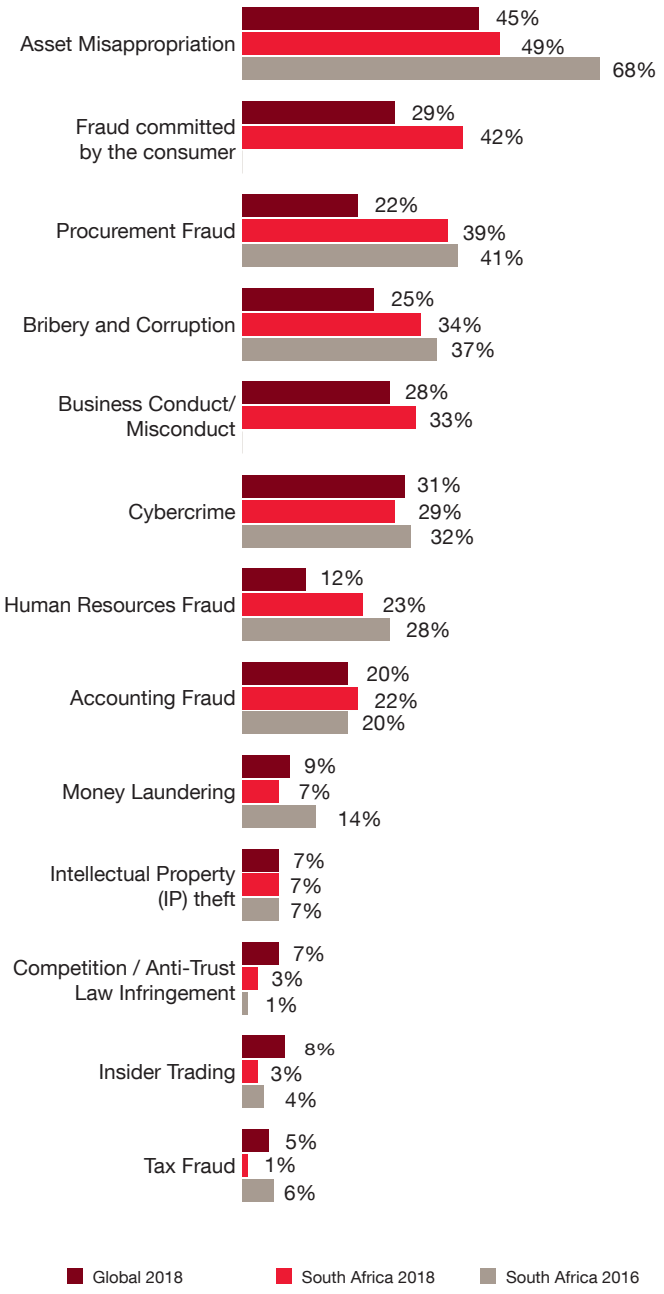
Figure 03: The reported rate of economic crime by region



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

Types of economic crime

Figure 04: Types of economic crime/fraud experienced

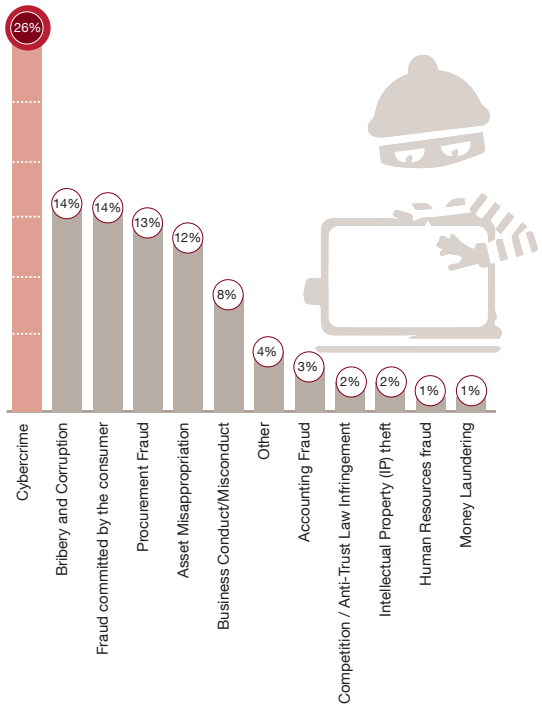


Q. What types of fraud and/ or economic crime has your organisation experienced within the last 24 months?

While asset misappropriation retained its top spot in the rankings, every category of economic crime types showed diminished instances of occurrence in comparison to 2016, with two exceptions: instances of accounting fraud increased to 22% (2016: 20%) and those of competition/ anti-trust law infringements increased to 3% (2016: 1%).

Surprisingly, while the instances of reported cybercrime showed a small decrease in the South African context, it retained its second place in the global rankings, albeit at a lower rate of occurrence than 2016.

Figure 05: Most disruptive economic crimes likely to be experienced over the next 24 months

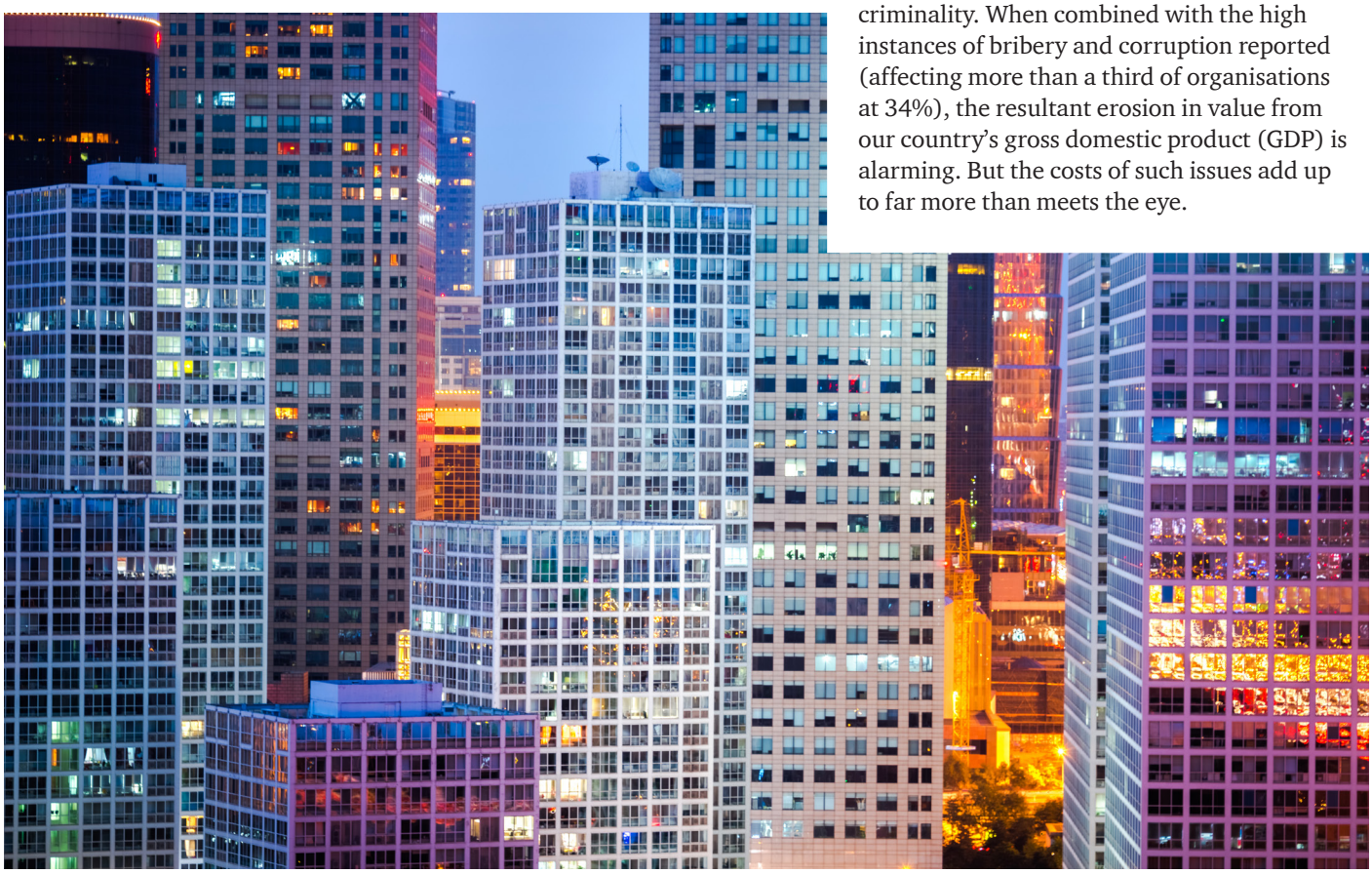


Q. Thinking about the next 24 months, which of the following fraud and/or economic crimes is likely to be the most disruptive/serious in terms of the impact on your organisation (monetary or otherwise)?

That having been said, more than a quarter of South African respondents (26%) believe that cybercrime will be the most disruptive economic crime to affect their organisations over the next 24 months.

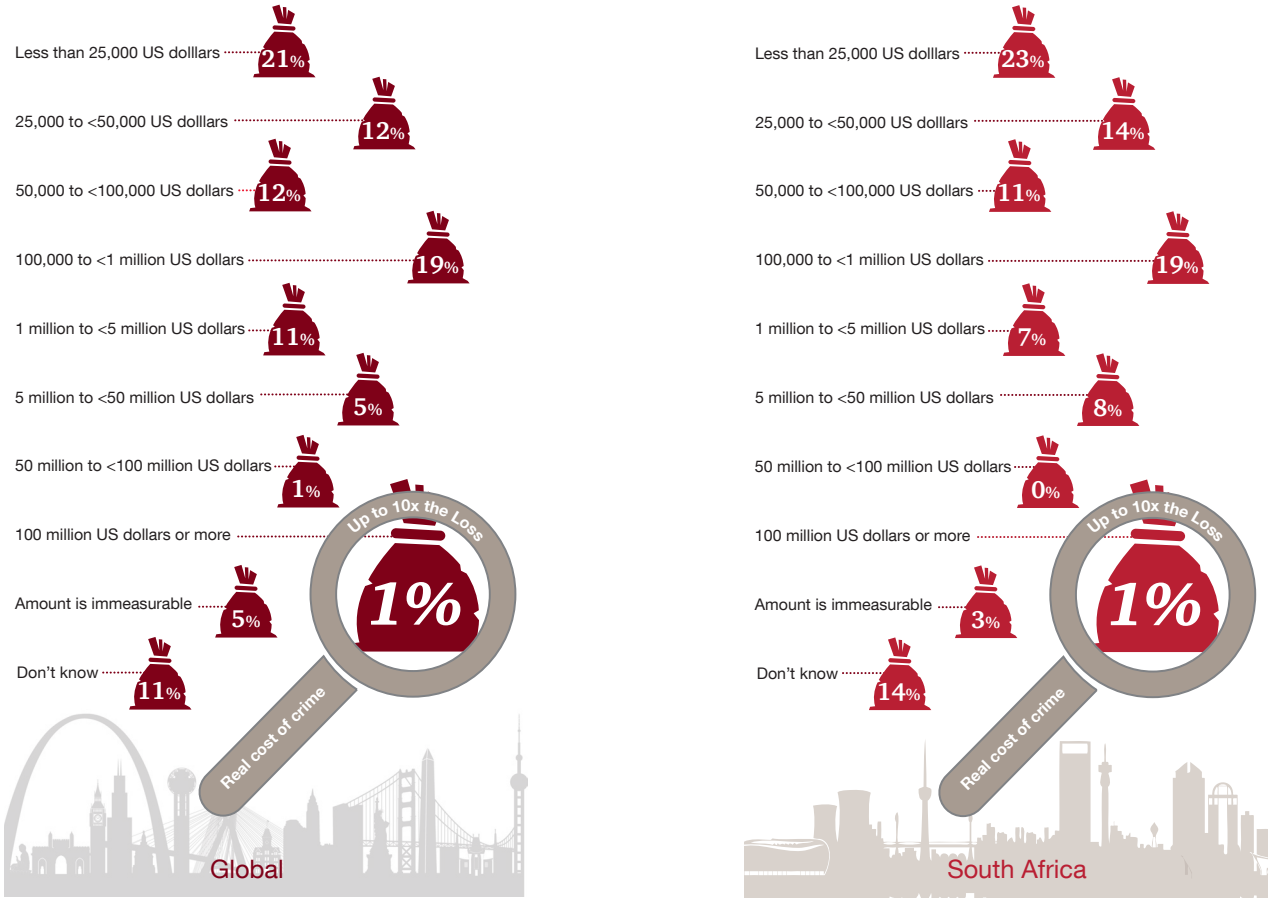
One of the new entries into the bank of options for the types of economic crimes experienced by organisations for the 2018 survey was that of 'fraud committed by the consumer'. This category was a consolidation of frauds traditionally committed by the end-user, including mortgage fraud, credit card fraud, claims fraud, cheque fraud, synthetic ID fraud and the like.

This particular crime, which highlights the propensity of the 'man in the street' to be a perpetrator of economic crime, makes one look with new eyes at who the victims of economic crime are. At second place in the South African ranking (with 42% of respondents having experienced this crime) and third place globally, fraud committed by the consumer also saw 20% of those respondents indicating that this fraud was the **most disruptive type of economic crime** experienced, followed closely by procurement fraud (at 19%). This shows that the entire supply chain in South Africa is fraught with criminality. When combined with the high instances of bribery and corruption reported (affecting more than a third of organisations at 34%), the resultant erosion in value from our country's gross domestic product (GDP) is alarming. But the costs of such issues add up to far more than meets the eye.



Cost of losses to economic crime and investigations

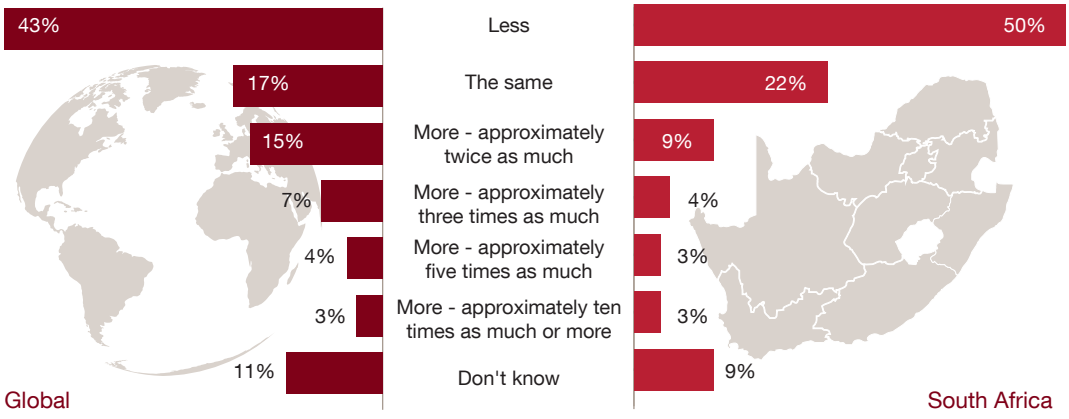
Figure 06: Financial impact of economic crime



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

35% of South African respondents lost more than $100,000 (+/- R1.2 million) to what they regarded as the most disruptive economic crime to affect them, with 1% reporting losses of greater than $100 million (R1.2 billion). When combined with the costs to address this issue through investigations or other interventions, where 41% of respondents reported having had to spend an equal or greater amount (10% reported having to spend upward of three times the amount, with 3% spending as much as ten times the value of the initial loss), we are faced with the damning realisation that the actual cost of these crimes is crippling our economy.

Figure 07: Extent of expenditure on investigating or other interventions to address the most disruptive economic crime/fraud



Q. As a result of the most disruptive crime experienced in the last 24 months, was the amount spent by your organisation on investigations and/or other interventions, more, less or the same as that which was lost through this crime?

This adds fuel to the argument that the costs to proactively implement preventative measures to counter fraud, while seeming unpalatable prior to a fraud occurrence, fade in comparison to the true cost of economic crime. These measures are not only necessary for prevention, but may be a vital ingredient for the survival of a business. So ask yourself – can you really afford to be *reactive* to economic crime? Our findings are rather clear on what the answer should be!

Fighting the good fight, or a losing battle?

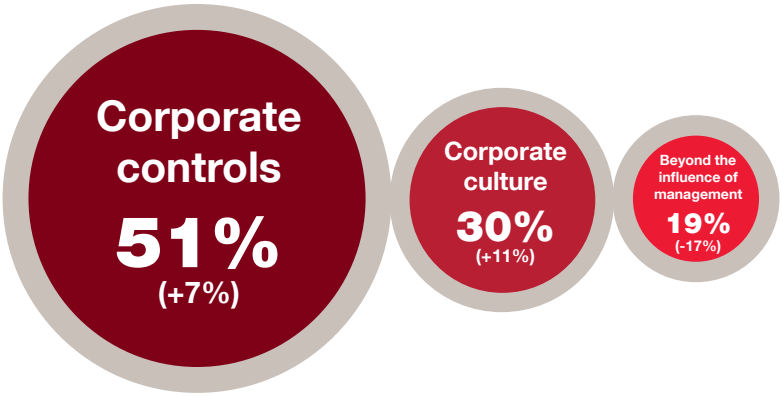
South African companies continue to invest in fighting the challenges that fraud and economic crime introduce into the business dynamic. 44% (Africa 41%) of respondents have increased their spend on combating fraud since 2016 and 46% plan to increase their spend over the next 24 months (Africa 45%).

This is good news – increased technology and analytics result in stronger internal controls, which translates into a newfound focus. This is further fortified by organisations reigniting their whistleblower programmes, which have in recent years seen a decline. Detection of wrongdoing through means of tip-offs and whistleblowing mechanisms remained strong this year, and our survey showed that almost two-thirds (64%) of South African respondents monitor whistleblower lines as a means to ensure the effectiveness of their compliance and governance programmes (Africa 51%). This represents a 9% increase since 2016.

What is even more reassuring is that business leaders are taking an active interest in their governance responsibilities and are becoming aware of, or rather want to be made aware of, the effects and issues that economic crime and fraud have on their organisations. 95% of South African respondents (versus 91% of Global and 94% of African) told us that the most disruptive incidents of economic crime were brought to the attention of the board executives or governance leaders within their organisations.

So how were the frauds detected?

Figure 08: Detection of the most disruptive economic crimes/fraud



Includes
Internal audit (routine) **9%**
Fraud risk management (general controls) **18%**
Suspicious activity monitoring **11%**
Corporate security (both IT and physical security) **5%**
Data Analytics **6%**
Rotation of personnel **2%**

Includes
Tip-off (internal) **14%**
Tip-off (external) **8%**
Whistleblowing hotline **8%**

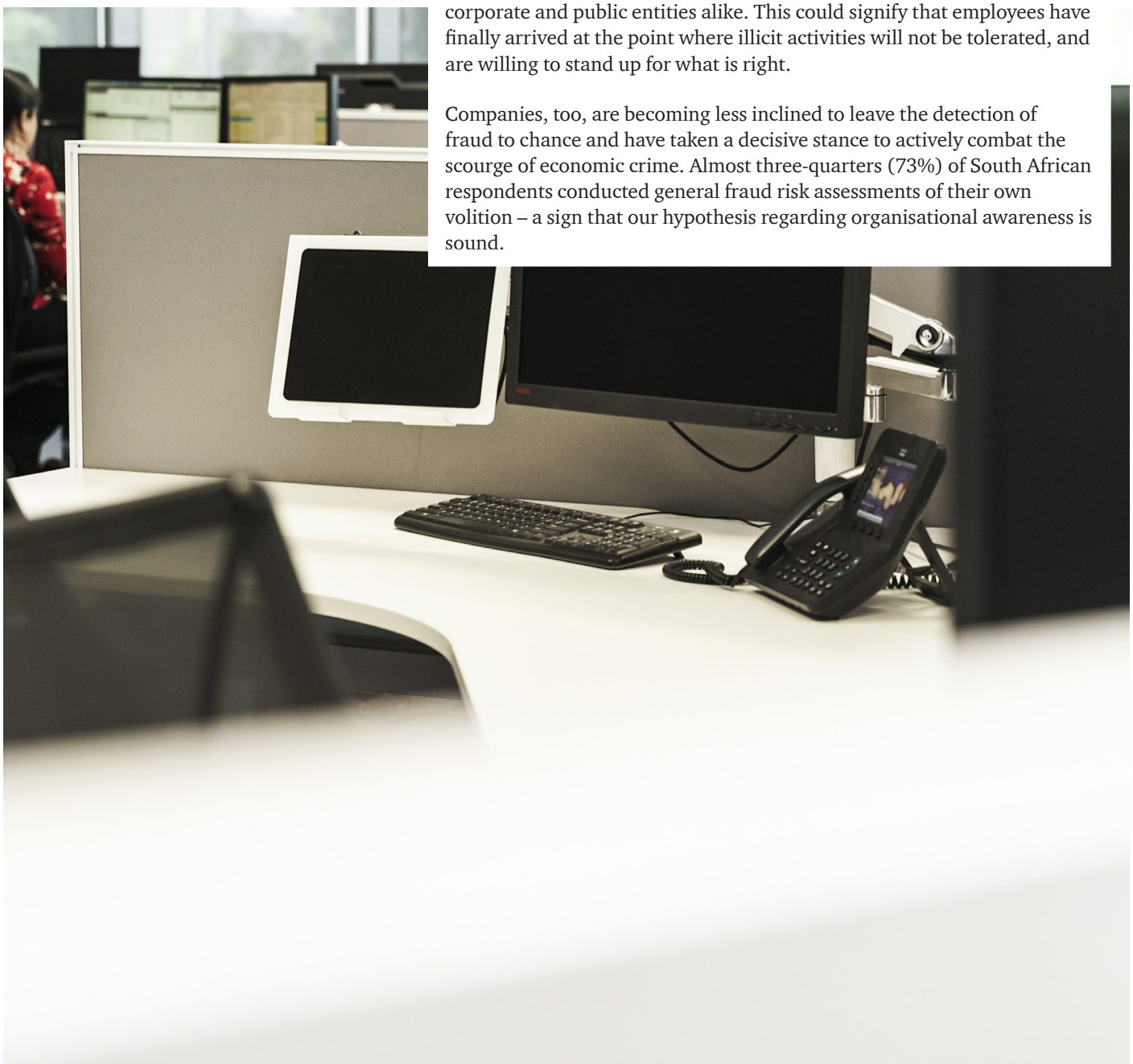
Includes
By accident **8%**
By law enforcement **2%**
Investigative media **3%**
Other detection method **5%**
Don't know **1%**

Q. How was the incident of the most disruptive fraud and/or economic crime that your organisation experienced initially detected?

It is quite uplifting to note that South African organisations have taken an active stance in assuming control of the detection of fraud, with the detection of fraud beyond the influence of management having declined by 17% since 2016.

Our findings indicate a shift in thinking whereby organisations are making better use of fraud risk management (18% – more than twice the instances noted in 2016) and data analytics to detect criminal activity. At the same time, it appears that the environments within organisations have become more receptive to trusting internal tip-off processes, as witnessed by the upsurge in the detection of fraud by means of internal tip-offs (14% compared to 6% in 2016). This is a further feather in the cap of corporate governance in that employees trust that management will do the right thing, and society is becoming an active agent of change for both corporate and public entities alike. This could signify that employees have finally arrived at the point where illicit activities will not be tolerated, and are willing to stand up for what is right.

Companies, too, are becoming less inclined to leave the detection of fraud to chance and have taken a decisive stance to actively combat the scourge of economic crime. Almost three-quarters (73%) of South African respondents conducted general fraud risk assessments of their own volition – a sign that our hypothesis regarding organisational awareness is sound.



The dawn of proactivity – get on board or get left behind

The need for moving toward proactively managing fraud risk has been an oft-repeated mantra of the anti-fraud community, and our findings of greater transparency and more committed, involved leadership in organisations may point to some hope in this arena.

But the rub of it is that with law enforcement and regulatory bodies across the globe increasingly moving toward active (and oft-times, unforgiving) enforcement, the trend may very well be a knee-jerk reaction to a desire by organisations to simply not be found wanting by the powers that be. Yet this could be a rare case of the end fully justifying the means.

But if we remain creatures that are compliant only because we are watched, the fight against fraud is lacking some vital ingredients, such as will. This makes for blind spots – lethal kinks in our armour.

Blind spots – what are we missing?

It is time for honest organisational introspection so we can emerge stronger and more effective in the global fight against economic crime and fraud.

While no one can deny that the enemy is at the gates, an interpretation of our results is that South African organisations are more aware than their global colleagues of the scourge of fraud and economic crime. Yet this challenge is exacerbated by the vulnerability of organisations to 'blind spots' – the cracks found in the overall awareness or responsibility matrix of even the most successfully run businesses. These cracks, which usually only surface after major incidences, are essentially a manifestation of the 'not my job' syndrome and of silo mentalities.

Fraud is defined by Oxford as '*wrongful or criminal deception intended to result in financial or personal gain*', but if you were to ask around the boardroom what fraud means to the individual executives charged with the responsibility of managing the various moving parts that make up an organisation, you will get very disparate views. The waters get even murkier when you start talking about responsibilities. A fragmented idea of responsibility is what creates the gaps where fraud festers, and this has devastating effects on the overall effectiveness of your fraud prevention efforts, regulatory outcomes and, ultimately, your financial performance.

Conversely, in operating in unison and throwing light on those blind spots lies great opportunity for companies to proactively fill the cracks and deliver a significant blow to fraud and economic crime.

Levels of detection still being outpaced by fraud risk

The rules are changing for businesses, profoundly and irreversibly, with tolerance for corporate and/or personal misbehaviour vanishing. Not only is public sensitivity about corporate misconduct at an all-time high; in some cases, corporations and leaders are also being held responsible for past behaviour, when the 'unspoken rules' of doing business might have been more lax.

PwC's 21st CEO Survey underscores this theme, with chief executives citing trust and leadership accountability as two of the largest business threats to growth.

All of this points to a heightened risk of incidents of fraud or economic crime occurring, and to a need for organisations to take the lead in preventing it before it can take root.

Since our last survey, we have seen some progress in the number of fraud detection measures taken by respondent companies. This is a good thing: not only can a fraud risk assessment help you identify the unique and specific fraud risks you should be looking for, but these assessments are increasingly favoured by regulators in enforcement actions.

83%

of South African CEOs agree or strongly agree that organisations are currently experiencing increased pressure to hold individual leaders accountable for any organisational misconduct (compared to 59% globally) and 71% are concerned about the lack of trust in businesses

Source: PwC 2018 21st CEO Survey

Still, our survey shows there is significant room for improvement. Only three in four South African organisations said they had conducted any kind of fraud or economic crime risk assessment. This correlates with the 23% of organisations that believe they haven't been touched by fraud – is this a coincidence?

Shockingly, only around a third (37%) of respondents had conducted an anti-bribery/anti-corruption risk assessment. This is an especially worrisome statistic, considering how impactful and expensive this crime has become worldwide on both the regulatory and financial sides.

Regulatory risk continues to grow

Across the board, regulations and reporting requirements, touching on both legal and ethical behaviour, continue to expand. Scrutiny and enforcement are also on the rise globally, and cross-border regulatory cooperation is becoming increasingly routine.

Thirty-six per cent of respondents involved in the business of money movement or financial services indicated that they had experienced a regulatory enforcement or inspection related to anti-money laundering (AML) in the last two years.

South Africa is undoubtedly undergoing far-reaching changes and visible enforcement is on the rise. 71% of our respondents expect recent changes in the geopolitical regulatory environment to have an increasing impact on their organisations in the next two years, and 63% of them expect more changes as regards the enforcement of regulations.

68%

of South African CEOs measure trust between their workforce and their organisation's senior leadership

Source: PwC 2018 21st CEO Survey

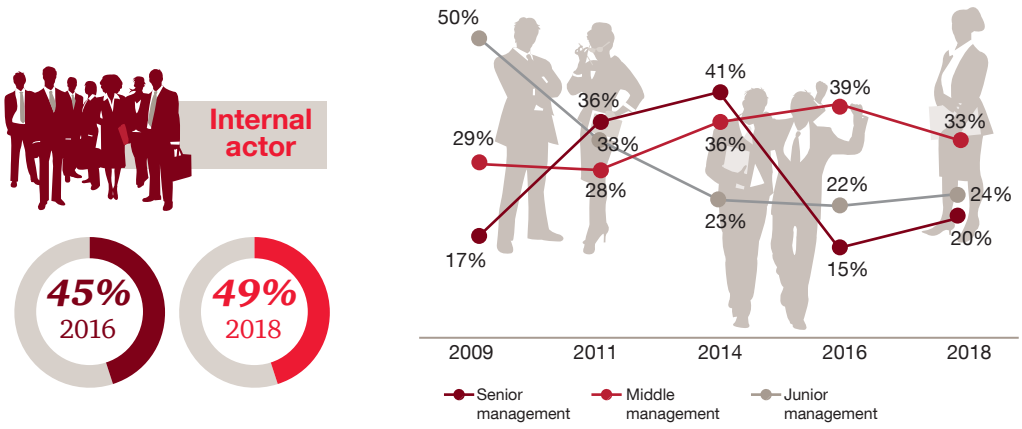
And what about acquisitions and other transactions?

In light of recent events, the risk of 'buying' successor liability and bad controls is at an all-time high. In these cases, a fraud risk assessment is even more critical as part of pre-deal due diligence.

Such enhanced due diligence is as critical to the acquiring company as it is to the private equity sector, which not only needs to rely on a clean bill of health on the investment side but would also need to tout it when selling an asset. Enhanced fraud, cybercrime and anti-corruption due diligence will allow acquirers to know what risks they face and how they can either be carved out of a deal or remediated post-deal. Furthermore, the results of both can increase the return on the sale side.

Meanwhile, many regulators are sharpening their scrutiny of conduct at the top and rightly so, given recent events unfolding in both corporate and government spheres. Whether it's due to an increase in awareness or an increase in misconduct, our survey revealed a significant bump (4%) in the share of economic crime committed by internal actors. In particular, there has been a 5% jump in the percentage of those crimes attributed to senior management, with one in five internal crimes now being committed by the custodians of organisations.

Figure 09: Internal perpetrators of economic crime/fraud



Q. Who was the main perpetrator of the most disruptive economic crime/fraud?

Developing nations setting the pace

Our survey shows that 58% of financial services respondents in developing countries underwent regulatory enforcement and inspections related to anti-money laundering in the last two years, compared to only 49% in developed countries.

When it comes to expectations of future anti-fraud investments, 15% of companies in developing countries expect to significantly increase funding in the next 24 months. By comparison, only 10% of respondents in developed countries plan to do so.

Fraud takes centre stage

Over the last few years we've seen a pronounced shift in the way the world looks at the perpetual issues of fraud and corruption. Our survey data reflects this deep undertow of a demand, both public and regulatory, for accountability, across both the private and public sectors.

This phenomenon is not limited to developed markets. Across vastly different cultures, in every region of the world, we are seeing signs of convergence on standards of transparency and expectations of conduct, driven by both regulators and the public. In nation-states where the rule of law and transparency have traditionally been weak, we've also seen public outrage displayed in the streets — some politicians and business leaders have gone to jail, and governments have even been toppled.

For all the drama they bring, these kinds of scandals are not outliers; they're leading indicators of a larger trend. The demands for accountability aren't stopping at the front door of headquarters. They've reached inside the building, all the way up to the C-suite offices and boardrooms.

Clearly, fraud risk has 'graduated' from being an operational issue to becoming a strategic business challenge that must be managed dynamically at the very highest level. With a risk landscape this fluid and fast moving, you can't rely on yesterday's profiles and methods to handle your anti-fraud measures.

20%

of reported internal frauds were committed by senior management

The jury of public opinion: Reputational risk now outstrips regulatory risk

Based even on fragmentary information, an organisation can find itself being punished from all corners for its perceived inability to respond appropriately to an issue — well before the board has a plan on what to do.

That's because, in the era of radical transparency, companies often don't get to decide when an issue becomes a crisis. The jury of public opinion does. As we are currently experiencing in South Africa, society's rules change faster than regulators', and there is little tolerance for those who don't follow them.

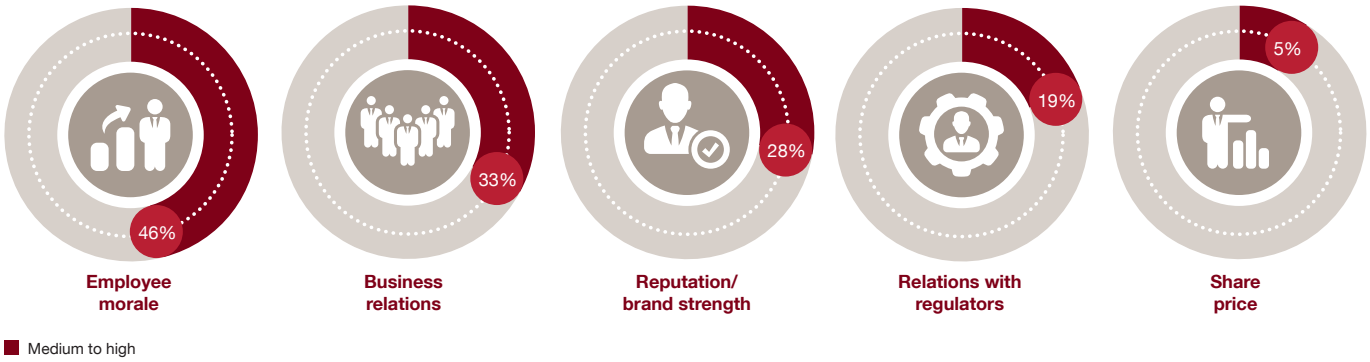
This year, we introduced a new category of fraud: business misconduct. This refers to fraud or deception perpetrated by companies upon the market or general public, and includes deceptive practices associated with the manufacturing, sales, marketing or delivery of a company's products or services to its clients, consumers or the general public. The significant number of respondents (33%) who confirmed that they had suffered just such a type of fraud suggests that this problem is far more widespread than is apparent from the high-profile business frauds splashed across the headlines.

Survey respondents have consistently ranked employee morale, business relations and reputation/brand strength among the top three elements that are vulnerable to the negative impacts of economic crime. These, coincidentally, have a direct effect on public perception from both within and outside an organisation.

This is not, of course, to minimise regulatory compliance, which, if anything, is more critical than ever. But consider that regulators, by definition, operate within a limited jurisdiction and under well-defined rules. A company's brand/reputation, on the other hand, is subject to no fixed jurisdiction, law or due process, as has been experienced recently in South Africa – even allegations that are later found to be incorrect can have negative results, and organisational survival hangs in the balance if perceptions are not managed appropriately and swiftly.

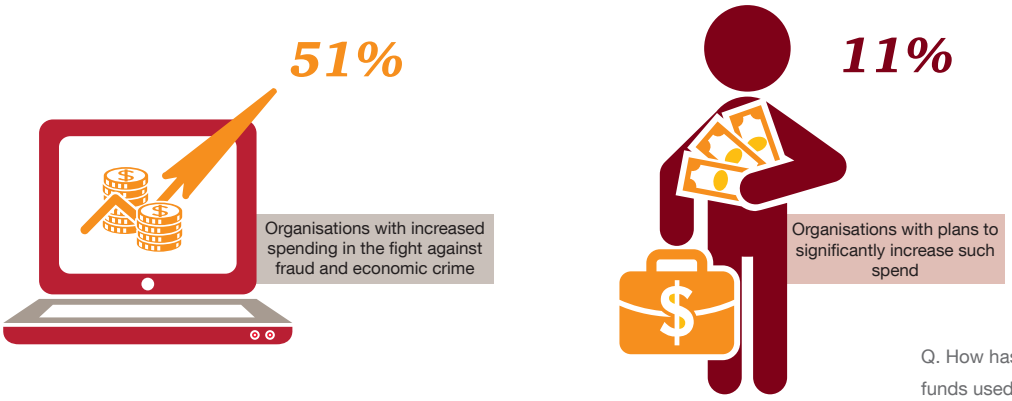
The desire to contain reputational damage is likely one reason why most companies are choosing to spend as much or more on investigations and other interventions as the loss experienced from the crime.

Figure 10: Impact of economic crime and fraud on business elements



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

Figure 11: Current and future spend on fighting economic crime/fraud



Q. How has/ is your organisation adjusting the amount of funds used to combat fraud and/or economic crime?

In light of investigating fraud costing up to ten times as much as the fraud itself, potentially amounting to millions of Rand – are we not still being too reactive?

Rightly or wrongly, the CEO and board are accountable

Our survey underscores that the cost of fraud — and of its aftermath — is substantial.

When the financial costs of fraud hit the bottom line, it's natural for senior management to be brought to account by the board and shareholders. Today, that responsibility doesn't stop there: it begins there. Chief executives are increasingly seen as the personal embodiment of an organisation, expected at all times to have their finger on the pulse of every facet of its culture and operations. And when ethical or compliance breakdowns happen, business leaders are often held personally responsible — both in the court of public opinion and, increasingly, by regulators.

Whatever the merits of such an aggressive response, the C-suite can hardly claim ignorance as an excuse. Our survey shows that almost every serious incident of fraud had been brought to the attention of senior management (95%). Furthermore, of the 85% of South African respondents who indicated their organisation had a formal business ethics and compliance programme, 21% said the CEO had primary responsibility for it. This puts a sharp spotlight on how the front office is managing the crisis — and the extent to which they are (or are not) adjusting their risk profiles accordingly.

Can you really change society by always playing by the rules?

Many companies are finding themselves caught in a tug of war between three business drivers: the market's appetite for innovative disruptors; shareholders' desire for financial outperformance; and society's expectations for ethical conduct.

The truth is that when businesses misbehave, investors often tend to look the other way as long as their investment is not threatened. The C-suite should be careful not to do the same. We often see that organisations can easily be lured into a false sense of security when scenarios appear to be rosy and when the 'tone at the top' appears to consist of the right words. What really counts is not the tone at the top, but the action at the top.

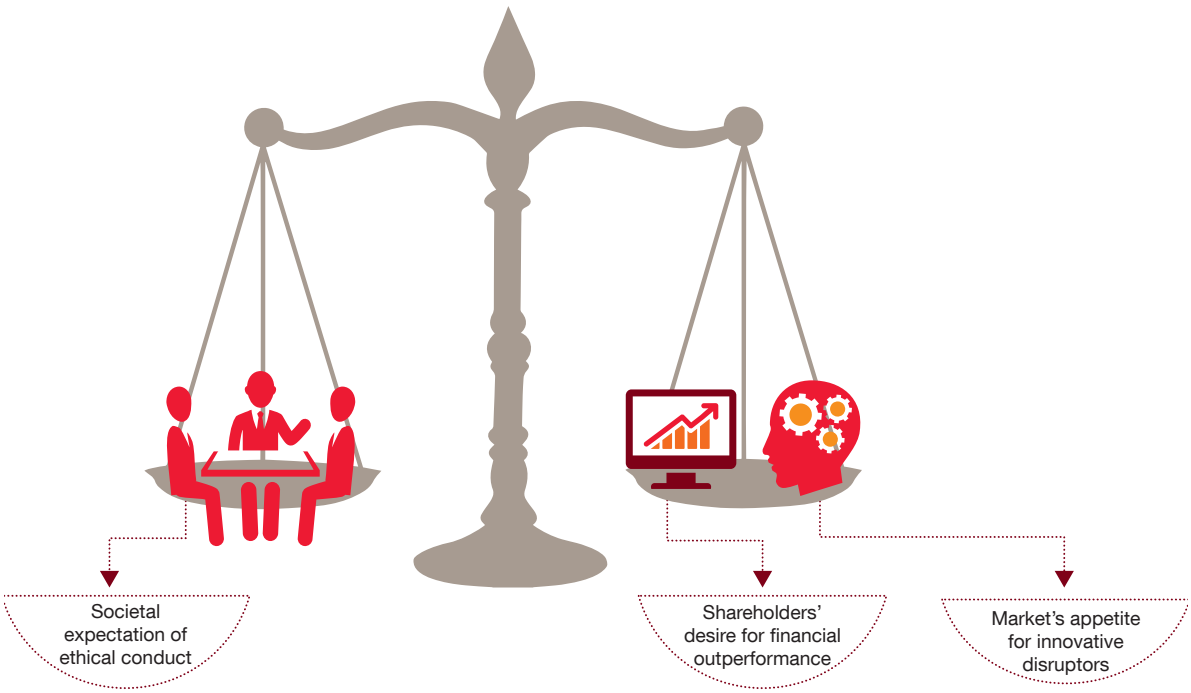
The market may love disruptors or outperformers — but not enough to tolerate bad behaviour. No matter how much of a stockmarket darling a company is today, if every aspect of conduct risk has not been managed carefully and soberly, both company and leadership could lose much of their goodwill faster than they acquired it. And South Africans have witnessed many a house of cards come tumbling down in recent times.

There is plenty of promise, however, among the start-up generation. Many of these fast-growing firms are led by younger entrepreneurs with an ethical viewpoint entrenched within their genetic composition. Unburdened by legacy processes or poorly integrated systems, they are ideally positioned to embed up-to-date fraud data analytics from the start — a tremendous competitive advantage in an era of multiplying frauds. These fresh-faced firms could help model a new era of both transparency and profitability.

85%

of South African respondents indicated their organisation had a formal business ethics and compliance programme

Figure 12: A formidable balancing act



Master the small challenges … and learn to weather the perfect storm

Breakdowns and mishaps are unavoidable. Yet the data suggests that there is plenty of upside to learning how to leverage small shocks. You could look at them as a blessing in disguise — an opportunity to test your systems and make improvements.

Part of the maturing process — for companies as well as countries — comes from weathering storms. According to a global study, *PwC's CEO Pulse on Crisis 2016*, when a crisis or unplanned event is well managed, 83% of CEOs report experiencing no negative impact on revenue growth. Beyond revenue, how the C-suite deals with what can become a crisis will be the measure by which it will be judged.

It is natural for a relatively inexperienced company to have a knee-jerk response to a crisis that blindsides it. Gradually, however, the company gains the 'muscle memory' that enables it to become more proactive, with mature ethics and compliance programmes and a battle-tested front office.

These are the circumstances that can help you stay above the noise, own the narrative, and emerge stronger — no matter what the future has in store.

83%

of CEOs report experiencing no negative impact on revenue growth, when a crisis is well managed

Source: PwC CEO Pulse on Crisis 2016

Today's technology as a tool to fight today's fraud

Fraud detection is not just a control, it is a vital business issue

When it comes to fraud, technology can be a double-edged sword, acting as both a business threat and a business protector. These areas traditionally resided at the operational level of the business, forming its second line of defence.

But technology has become so pervasive across every business process, including customer-facing areas, that how you leverage it to combat fraud — the balance you strike between safety and overzealousness — is now central to the customer experience. And that makes it a vital issue for senior management as well.

Fundamentally, companies are realising that fraud, regardless of how it manifests, is first and foremost a *business* problem which could seriously hamper the growth agenda. In response, many have made a strategic shift in their approach to external fraud, and are making a business case for robust new investments in areas such as detection, authentication and reduction of customer friction*.

21%

of respondents said they thought their organisation's use of technology to combat fraud and/or economic crime was producing too many false positives

*What is customer friction?

When customers get too many false fraud alerts from a bank or vendor, their first reaction is generally not one of gratitude for superior information security – it is annoyance. This is customer friction. And it is a growing challenge for organisations as they seek to strike the right balance between acting on fraud red flags, and being overzealous in sending alert communications to their customers.

This is a tight spot to be in — and the margin for error is not large. On the one hand, you run the risk of missing a fraudulent transaction (with the financial and reputational fallout that follows). On the other, as our survey shows, you risk alienating (and losing) your customer base: more than one in five South African respondents (21%) said they thought their organisation's use of technology to combat fraud and/or economic crime was producing too many false positive alerts.

Adopting fit-for-purpose tech

On the fraud defence front, organisations today have available a wealth of innovative and sophisticated technologies aimed at monitoring, analysing, learning and predicting human behaviour. And the data shows they are using them in varying degrees, depending on sector.

Technology can be prohibitively expensive to buy and adopt across a large organisation. And the decision regarding what to purchase, and when, is a delicate one. Some organisations invest in emerging or disruptive technologies that they don't use optimally. Others jump in too late and find themselves behind the curve in the struggle to catch fraud or flag potential trouble spots.

Our survey shows, surprisingly, that companies in emerging markets, including South Africa, are actually investing in advanced technologies such as artificial intelligence at a faster clip than developed nations — possibly as a way to catch up in an area where other nations have already sunk considerable infrastructure cost. Either way, it's clear that the use of innovative technologies to combat fraud is now a worldwide phenomenon.

The wide reach of technology and the stealthy growth of fraud are creating a double challenge for all organisations: finding the sweet spot between effectiveness and cost, and not getting outpaced by fraudsters that are also combining brain and machine power to go on the attack.

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

Your customers are the lifeblood of your business. As business models continue to evolve through the digital revolution, many are getting exposed to payment fraud for the first time. How you handle that fraud will profoundly affect your own outcomes.

Here are some of the characteristics and challenges of today's digital fraud:

New digital products are creating new attack surfaces. To bring products to market, companies once followed an established B2B process involving resellers, distributors and retailers. On today's innovative B2C digital platforms, there is a much wider attack surface — and much more room for fraud to break through.

Industry lines are blurring. In the digital economy we are witnessing a crossing over of some non-financial services companies into payment systems. Whereas financial services traditionally had the most advanced anti-fraud measures and the legacy knowledge of fraud and money-laundering risk, some of these relative newcomers to the payment space lack this experience and know-how, making them, and their third-party ecosystem, susceptible to both fraud and regulatory risk.

The technical sophistication of external fraudsters continues to grow. Digital fraud attacks continue to get more sophisticated, thorough and devastating. Consider how a single ransomware attack in 2017 crippled Britain's entire National Health Service (along with hundreds of thousands of computers the world over), putting lives at risk. Or how, in a 2016 hack, fraudsters managed to subvert several banks' SWIFT accounts — the international money transfer system that all banks use to move billions of dollars daily among themselves — stealing nearly US$100 million from the Bangladesh Central Bank.

You can change your credit card number, but you can't change your date of birth. The knowledge-based authentication tools long used to control fraud are outdated, but most companies haven't replaced them yet. When a national entity suffers a massive breach, what's stolen isn't a replaceable asset such as cash — but unique, deeply personal identity markers such as date of birth or social security number. Since this is the very data that's typically used to verify identity and prevent fraud, such a breach essentially opens the door for any fraudster to take over a person's identity. Unfortunately, many companies have not yet adopted the new techniques — such as digital device ID and voice biometrics — that have now become necessary to protect their customers' assets.

Cyber attacks: Through a smashed door or an open door?

Companies continue to cast a wary eye on cybercrime, with over a quarter of respondents not only expecting to experience a cyber attack in the next two years, but also believing it will be the most disruptive, impactful crime they will face. In fact, cyber attacks have become so inescapable that measuring their occurrences and impact is becoming less strategically useful than focusing on the mechanism that the fraudster used.

While all digital fraud is fraud, not all fraud is digital. So it can be helpful to delineate the two different ways one can look at cybercrime as either digital theft or digital fraud. The crime of digital theft could include stealing cash, personal information or intellectual property, and it could involve extortion and ransomware, or a host of other crimes. This type of crime can be likened to the stolen goods as opposed to the smashed door. Digital fraud, on the other hand, is where the fraudster penetrates an *open* door (typically, but not always, a customer- or employee-facing access point) and uses the company's own business processes to attack it. In many ways, this is the more malicious type of attack, and to combat this type of fraud, the organisation must use digital methods — both as a remedy against, and as a medicine for treating, the infestation.

Fraud detection moves up to the first line of defence

Where, traditionally, fraud prevention and detection would have been the domain of the organisation's second line of defence — risk management, legal, compliance, etc. — today's enterprises are increasingly embedding their newly reinforced fraud prevention measures into the fabric of their first line of defence.

Our survey results support this: 20% of respondents in South Africa indicated that the CEO (who is part of the first line of defence) has primary responsibility for the organisation's ethics and compliance programme, and is therefore more instrumental in the detection of fraud and the response to it.

This is likely just the beginning of a significant shift, where first-line fraud prevention and detection capabilities continue to mature and strengthen. As they do, they will enable the second line of defence to shift to a more traditional second-line approach — governance and oversight, and setting risk tolerance, frameworks and policies.

In a world where the boundaries between industries, technology and regulatory bodies continue to blur and where fraudsters are looking beyond the traditional, highly protected financial services targets for soft spots where they can ply their trade, this is an important development.

Figure 13: Lines of defence

Anti-money laundering (AML) obligations: not just for banks

Over one-third (34%) of our survey respondents indicated that their businesses were involved in money movement. Regardless of whether they are true financial services companies, one thing is clear: regulators will expect these companies to develop AML compliance programmes with defined degrees of monitoring and compliance. In fact, almost two-thirds (59%) of respondents told us they are subject to both international and local AML regulations, so the net is widening faster than one may think.

Non-financial companies may not have the same regulatory obligations as their financial services (FS) counterparts, but they too could find themselves running foul of the law. That's because regulators and law enforcement agencies are now looking beyond the primary impact of a crime such as, for example, trafficking in counterfeit goods to examine what illicit activities the stolen assets went to finance. And, as part of their remit, they are scrutinising non-FS companies' compliance and anti-fraud measures for signs that they may be, consciously or not, 'aiding and abetting' such criminal activities — a further illustration of the increasingly blurred boundaries between sectors when it comes to fraud prevention.

Fraud technology: The business case

The business case for investment in fraud technology goes beyond protecting against reputational, regulatory or financial damage. It also includes reducing the cost of fraud prevention through efficiencies, enabling you to safely build and sell new products and services on a digital platform; and fine-tuning your fraud programme to reduce 'customer friction'— allowing your good customers to interact more freely with your platform and your product, without excessive fraud prevention controls getting in the way.

Invest in people, not just machines

A small investment in people can pay huge dividends

Technology is clearly a fundamental tool in the fight against fraud, but it's not the only one. It may not even be the most strategic one. Confronted with the obstinate nature of fraud, many organisations opt to pour more resources into technology. Yet when it comes to fighting fraud (and, in particular, internal fraud) technology investments invariably reach a point of diminishing returns.

That's because fraud is the product of a complex mix of conditions and motivations, only some of which can be combated by machines or processes. The most critical factor — the 'last mile' to a bad decision — is human choice. And ultimately, focusing on human behaviour offers the best opportunity for reducing or preventing it, because, ultimately, machines don't commit fraud, people do – they just happen to be using technology more and more in these endeavours.

When it comes to cutting fraud off at the legs, the return on investment (ROI) on people initiatives is likely to far exceed that of another piece of technology.

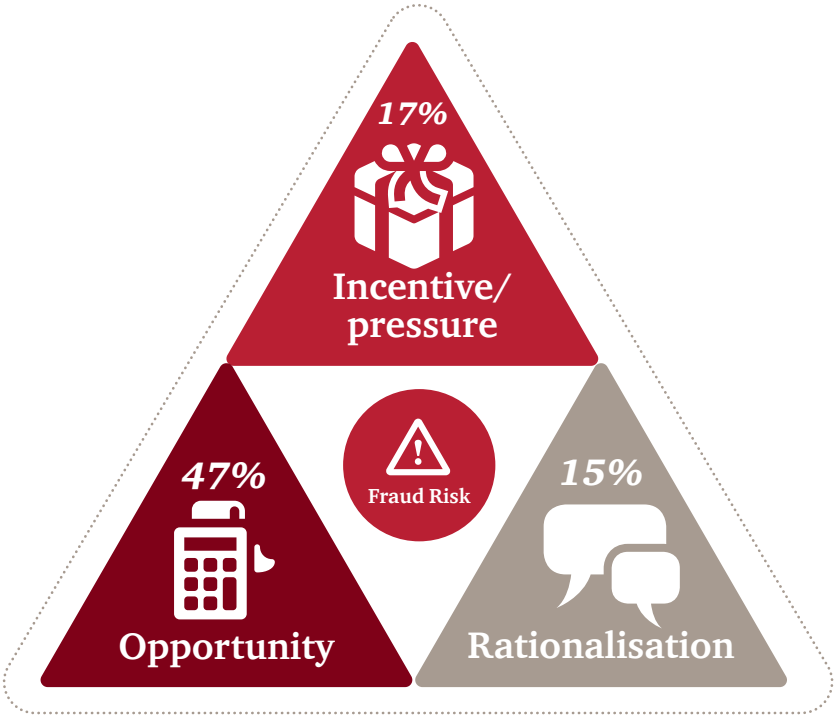
Controls and culture: The fraud triangle

An excellent way to frame the problem of internal fraud is to use a construct called the *fraud triangle*. It is a powerful method for understanding and measuring the individual drivers of internal fraud — and an ideal springboard for focusing on ways to prevent it, holistically.

The birth of a fraudulent act usually follows the following trajectory:
It starts with *pressure* – generally related to an internal issue. Then, if an *opportunity* presents itself, the person will usually wrestle with it emotionally. The last piece of the puzzle, which enables them to move from thought to action, is *rationalisation*.

Since all three of these drivers must be present for an act of fraud to occur, all three need to be addressed individually, in ways that are appropriate and effective.

Figure 14: The Fraud Triangle



Q. To what extent did incentive, opportunity and rationalisation contribute to the incident of fraud/ or economic crime within your organisation committed by internal actors?

The antidote to opportunity: controls

Of the three sides of the fraud triangle, the bulk of the effort over the years has gone to addressing the *opportunity* to commit fraud — with 71% of South African respondents indicating that they expend a high degree of effort in building up business processes such as internal controls, which have gotten steadily more sophisticated. Our survey clearly reflects the results of this prioritisation, with the relative share due to opportunity dropping from 72% to 47% in only two years.

Unfortunately, companies are putting significantly less effort into measures meant to counteract pressures and rationalisation, with only 42% of respondents indicating that they spend a high level of effort promoting ethical decision-making by individual employees. Here again, we see the results of these choices: 17% of respondents ranked incentive/pressure as the leading factor contributing to the most disruptive fraud committed by internal actors, a 6% increase from 11% in 2016. Rationalisation showed a similar trend, with 15% of respondents indicating that this was the leading motivating factor to commit fraud (up from the 10% reported in 2016).

This under-emphasis of culture/ethical measures points to a potential blind spot and may be one reason why internal fraud is so resilient. Because fraud is the result of the intersection of human choices with system failures, it's important to be wary of the false sense of security that internal controls, even well-designed ones, can bring.

But here's the problem: almost half (49%) of respondents indicated that an internal actor was responsible for committing the most disruptive fraud. And addressing internally committed fraud requires more than technology and processes; it requires a focus on the *culture* driving or enabling the internal misbehaviour.

The antidote to pressure: openness

To embed a process that encompasses the full spectrum of fraud risk, you have to look beyond the opportunity/controls nexus, and take both a wider and deeper look inside.

Corporate-sized frauds are generally connected to corporate pressures — and the *pressure* to commit fraud can arise at any level of the organisation. At the highest level, such pressure can include a seemingly altruistic desire to save the company by hitting key funding targets or otherwise satisfying external expectations. In the middle ranks of the organisation, these pressures can manifest as unrealistic sales expectations, poorly designed compensation structures, unreasonable supervisors, or a desire to recoup or avoid losses.

It is important not to over-emphasise the importance of financial incentives when considering what might drive a person to commit fraud. Generally, the motivation is not money, but fear and embarrassment — fear to admit to making a mistake, the need to lie to cover it up, with the hole deepening at each turn. With this in mind, examine the pressures and incentives coming from the top, beyond the expected financial results: Are they complying with regulations? Are they consistent with doing the right thing for customers and people?

Short-term tailored controls can serve as a check on whether aggressive sales programmes are leading to fraudulent or illegal behaviour. And a well-publicised open-door or hotline policy can help, too — not only as a pressure-release valve, but also as an early-warning system of potential problems down the line.

49%

of respondents indicated that an internal actor was responsible for committing the most disruptive fraud

The antidote to rationalisation: culture

While pressure and opportunity can be influenced and controlled by the organisation (at least to some extent), the element of *rationalisation* is the wild card. That's because it lives, not on a computer, or in a procedural manual, but inside the mind of a human being.

The person who decides to commit an act of fraud against their own employer has reconciled their planned actions to their own personal code of ethics, and found a way to excuse (or rationalise) their intended behaviour. They do so because they think it won't hurt anyone, or it's 'for a good reason', or it will be rectified before anyone finds out, or they won't get caught.

This is a peculiarity of internal fraud: due to a lack of proximity, those who commit it often see it as a victimless crime — they cannot visualise the face of a human who has been directly harmed by the action.

So how to handle this, the most mysterious driver of fraud? We've found that the first step on the ladder is to focus on **understanding the environment** that governs employee behaviour. Using surveys, focus groups and in-depth interviews, probe it to find your internal culture's strengths and weaknesses, and focus on the areas that are lax or problematic.

Consistent training is also key. If people clearly understand what constitutes unacceptable actions — and the consequences of taking such actions — it will be that much harder for them to rationalise or justify fraudulent activity. Unlike our global counterparts, South African organisations have an inclination toward investing in training initiatives. In fact, the percentage of respondents who indicated they have a formal business ethics and compliance programme has increased from 80% to 85% since our 2016 survey. And we found that 71% of South African companies (compared to 58% of global respondents) with such a programme indicated their organisation has specific policies targeting general fraud.

Another effective solution is to have employees periodically sign compliance agreements confirming that they have followed company protocols. This kind of regular day-of-reckoning exercise can be a powerful deterrent to the rationalisation of bad behaviour. It can also serve as an audit trail if needed.

The problem with internal controls

One of the consequences of an over-reliance on technology is the belief that standard internal controls alone can catch fraud.

But there's a fundamental flaw in that model: it is based on the assumption that management will always behave ethically. In fact, experience shows that virtually every material internal fraud is a result of management circumvention or override of those very controls. And indeed, our survey reveals that more than half of serious internal fraud committed was perpetrated by senior and middle management (53%).

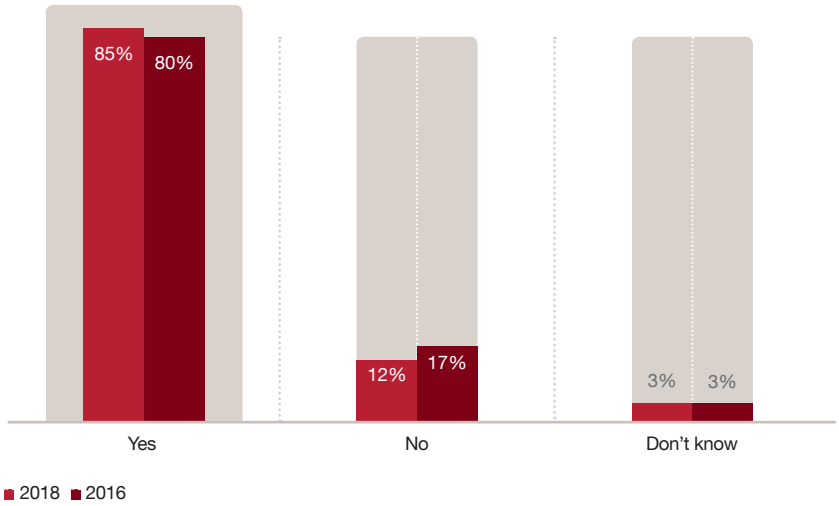
Addressing this fundamental structural problem requires overlaying your garden-variety controls with fraud risk controls customised to your unique business culture. That means creating controls that actually *plan* for management override or collusion in targeted areas.

The first step in this process is to conduct a fraud risk assessment of your organisation. Yet, considering how critical this step is in the fight against fraud, it is surprising that all organisations have not yet adopted this strategy.

Our survey reveals that over the last two years, 73% of respondents have conducted a general fraud risk assessment and 62% have assessed their vulnerability to cyber attacks. But only around one-third of respondents have performed risk assessments in the critical areas of anti-bribery and corruption and a cyber response plan, with less than a fifth of respondents having carried out assessments in the area of either AML or sanctions and export controls. One in 12 respondents has not performed any risk assessments at all in the past 24 months.

These numbers graphically illustrate the scope of this blind spot. But if you flip the lens, you can also read in them a hopeful fact: In the fight against fraud there is significant untapped potential.

Figure 15: Companies reporting having ethics and compliance programmes



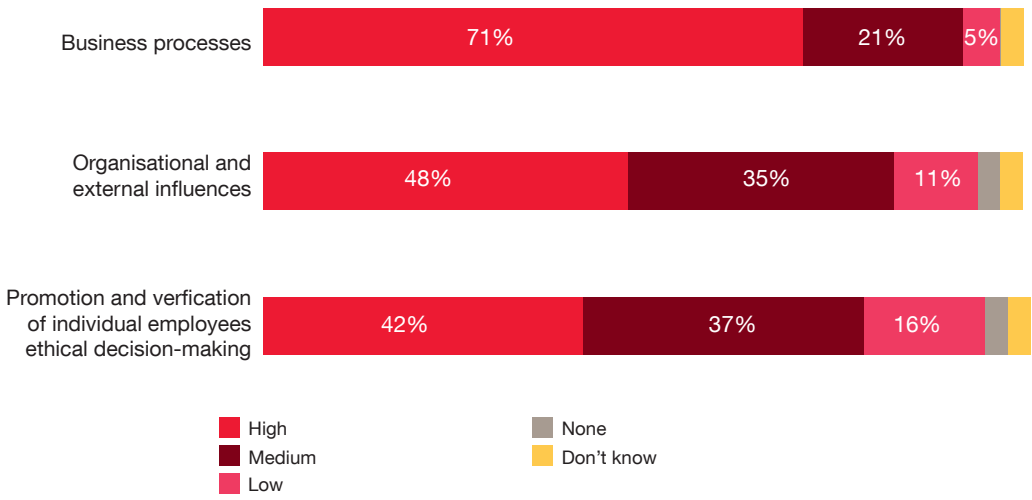
Q. Do you have a formal business ethics and compliance programme in your organisation?

Lower your 'fraud floor': Focus on your people

The task of allocating both energy and funds to a myriad elements that can detect and prevent economic crime or fraud is a complex one. Just as fraud does not happen through the agency of a single factor, but by a combination, you have to find the right formula of technology and people measures. Yet many organisations who have focused primarily on technology resign themselves to the belief that there is nothing more they can do — that a certain amount of fraud is simply part of the cost of doing business.

While fraud will always be with us, there are in fact many opportunities to lower your 'fraud floor'. When you consider the scale of losses caused every year by successfully committed acts of internal fraud, an investment in understanding and evolving your culture may offer a surprisingly high return, assuming you already have a well-established control environment. Our survey results clearly suggest that this is where companies should now redirect some of their effort.

Figure 16: Level of effort in specific areas to combat internal fraud



Q. What level of effort does your organisation apply to the following categories in order to combat fraud and/or economic crime internally?

Conclusion

Preparation is key – go on the offensive against fraud

Beyond offering valuable data on the evolution and current state of fraud among our nearly 300 respondents from South Africa alone, this year's Global Economic Crime and Fraud Survey sheds much-needed light on some of the most important strategic challenges confronting every organisation — from compliance, culture and crisis response to new perspectives on accountability, technology and cybercrime.

Throwing light on your blind spots can also unlock significant opportunities. It can help you effect positive structural improvements across the organisation — benefits which can make you stronger and more strategic in good times and bad. These improvements include moving away from silo views of functions like compliance, ethics, risk management and legal, and enabling a culture that is more positive, cohesive and resilient.

The value proposition of an up-to-date fraud programme may be hard to quantify, which can make it difficult to secure the needed investments. But consider the opportunity cost — financial, legal, regulatory and reputational — of not setting up a culture of compliance and transparency.

Recent events have demonstrated that not only has the threat of economic crime continued to intensify; the rules and expectations of all your stakeholders — from regulators and the public to social media and employees — have changed, irrevocably. Today, transparency and adherence to the rule of law are more critical than they have ever been.

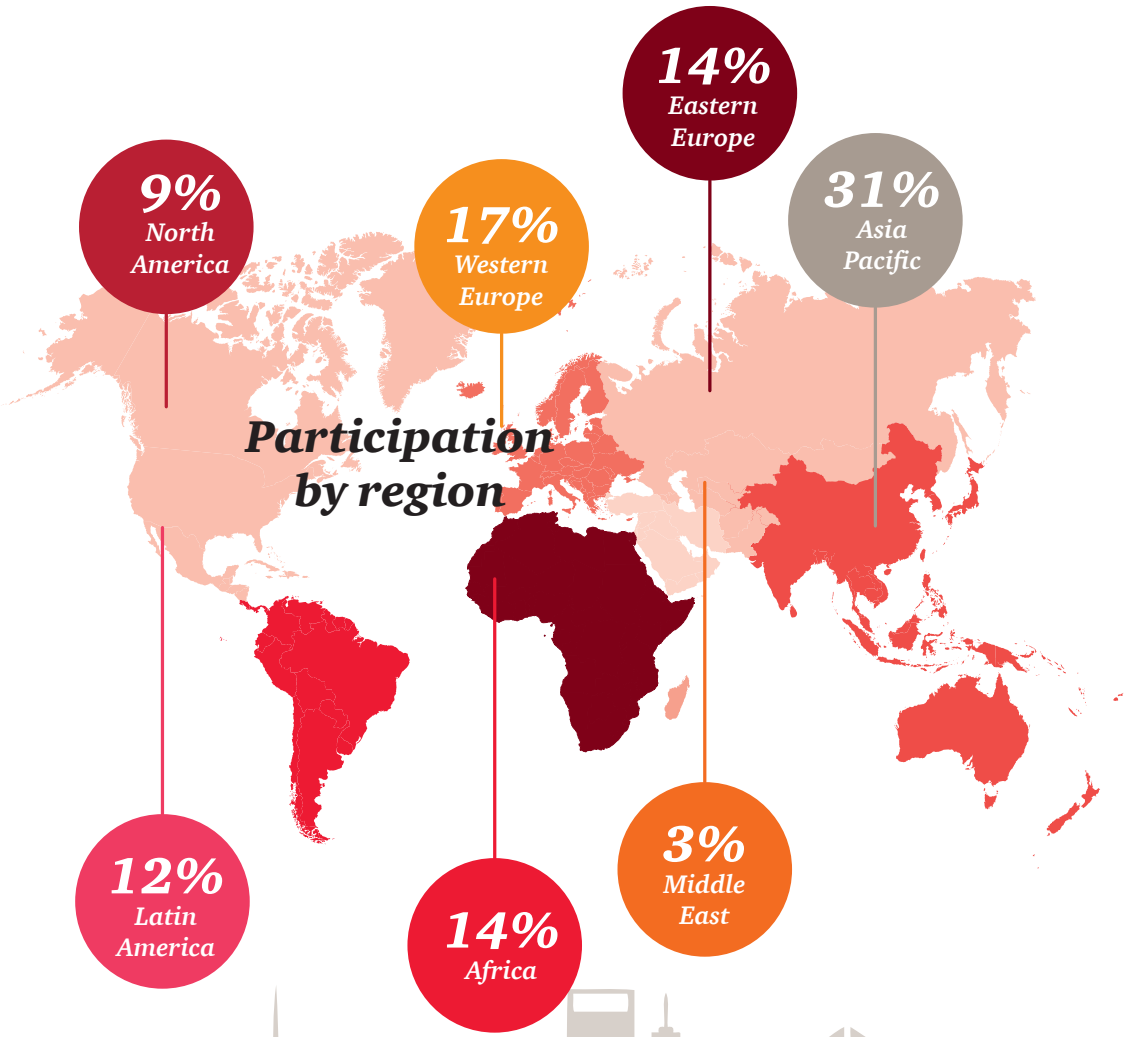
A Global Survey

7,228 Completed Surveys

123 Countries

Between **21** June and **28** September 2017

Surveyed in **18** Different Languages



Participation statistics

Respondents

282
South African respondents

73%
of respondents in Executive Management, Finance, Audit, Compliance or Risk Management

45%
of the survey respondents represented publicly traded companies

53%
of respondents were from multinational organisations

55%
C-suite

24%
Head of Department or Business unit

Industry sectors

33%
Industrial

18%
Financial Services

11%
Government & State-owned

10%
Consumer

5%
Agriculture

23%
Other

Contacts

Africa Forensic Services Leader

Louis Strydom
Partner, Johannesburg
+27 11 797 5465
louis.strydom@pwc.com

Southern Africa Forensic Services Leader

Trevor Hills
Partner, Johannesburg
+27 11 797 5526
trevor.hills@pwc.com

Forensic Investigations

Malcolm Campbell
Partner, Cape Town
+27 21 529 2676
malcolm.campbell@pwc.com

Gerhard Geldenhuys
Partner, Bloemfontein
+27 51 503 4106
gerhard.geldenhuys@pwc.com

Lionel van Tonder
Partner, Johannesburg
+27 11 287 0152
lionel.tonder@pwc.com

Trevor White
Partner, Johannesburg
+27 31 271 2020
trevor.white@pwc.com

Moazam Fakey
Associate Director, Johannesburg
+27 11 797 4750
moazam.fakey@pwc.com

Boitumelo Lekoko
Associate Director, Johannesburg
+27 11 287 0163
boitumelo.lekoko@pwc.com

Gerard Sutton
Associate Director, Port Elizabeth
+27 41 391 4422
gerard.sutton@pwc.com

Anti-bribery and Corruption

Trevor Hills
Partner, Johannesburg
+27 11 797 5526
trevor.hills@pwc.com

Global Intelligence

Chesirè le Roux
Associate Director, Cape Town
+27 21 529 2326
chesire.le.roux@pwc.com

Dispute Resolution & Litigation Support

Trevor White
Partner, Johannesburg
+27 31 271 2020
trevor.white@pwc.com

Louis Strydom
Partner, Johannesburg
+27 11 797 5465
louis.strydom@pwc.com

Greg Truter
Senior Manager, Johannesburg
+27 11 797 4661
greg.truter@pwc.com

Cybercrime & Forensic Technology Services

Junaid Amra
Partner, Durban
+27 31 271 2302
junaid.amra@pwc.com

Fraud Prevention Consulting

Josette Sheria
Partner, Johannesburg
+27 11 797 4111
josette.sheria@pwc.com

Financial Crime & Compliance

Kent Kirkwood
Associate Director, Johannesburg
+27 11 797 4807
kent.kirkwood@pwc.com

Roy Melnick
Associate Director, Johannesburg
+27 11 797 4064
roy.melnick@pwc.com

Christo Toerien
Associate Director, Johannesburg
+27 11 287 0875
christo.toerien@pwc.com

Kerin Wood
Associate Director, Johannesburg
+27 11 797 5246
kerin.wood@pwc.com

Survey management team

Moazam Fakey
Associate Director, Johannesburg
+27 11 797 4750
moazam.fakey@pwc.com

Liesl Opperman
Senior Manager, Johannesburg
+27 11 797 5276
liesl.opperman@pwc.com


pwc
VITA EXCLUSIVE
VITA EXCL

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers Inc, its subsidiary and associated companies and entities and their respective directors, employees agents and subcontractors do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2018 PricewaterhouseCoopers ("PwC"), the South African firm. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers in South Africa, which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity and does not act as an agent of PwCIL. (18-21654))