

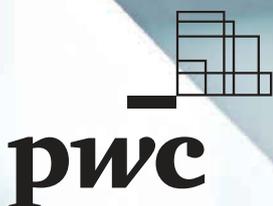
2020

Economic crime – When the boardroom becomes the battlefield

**PwC's Global Economic Crime
and Fraud Survey**

7th South African edition

March 2020



www.pwc.co.za



Contents

- 04 Leading observations
- 07 Foreword
- 08 **1** Fraud perspectives: When less is actually more
- 10 **2** Changing tides in the types of economic crime
- 12 **3** Redefining being bulletproof by looking inward
- 16 **4** Feeling the pinch: The cost of economic crime
- 18 **5** A wake-up call for boards and regulators
- 24 **6** Taking initiative: Preparing for fraud
- 26 **7** When the time comes, react the right way
- 28 **8** Rising from the ashes: Measuring success
- 30 Conclusion: The writing is on the wall
- 31 Contacts

Leading observations

Organisations are facing increased complexity – are you prepared?

20% to 34%

Fraud perpetrated by senior management up from 20% in 2018 to 34% in 2020.

22% to 34%

Accounting/Financial statement fraud up from 22% in 2018 to 34% in 2020.

One in five incidents featured internal and external perpetrators.

Cybercrime remains in the top five.

Value up, volume down – does this measure the complete cost?



Volume

60%

Incidents down from 77% in 2018 to 60% in the current survey.



Value

4%

4% report direct losses in excess of \$100 million (global: 7%).



Cost

- One in three South African respondents cite distrust as being the most significant emotional impact of incidents.
- Brand damage, loss of market position, employee morale, and lost future opportunities remain unquantified.

Is your fraud programme delivering what you think it is?

60%



of South African respondents that addressed a disruptive incident say their organisation emerged stronger.

Shockingly, however:

42%

of respondents didn't conduct an investigation

66%

of incidents were not disclosed to regulators or law enforcement

59%

of incidents were not disclosed to the board

72%

of incidents were not disclosed to the auditor

The demands are only increasing

- More scrutiny from broader stakeholders
- Almost half of respondents are planning to increase their spend on fraud prevention
- Speed of response will determine the containment of damages and losses



Global

5,000+



respondents

62%

of respondents were C-suite

72%

have US\$10M+ in global revenue

99

territories



US\$42B

in losses



South Africa

245



South African participants

71%

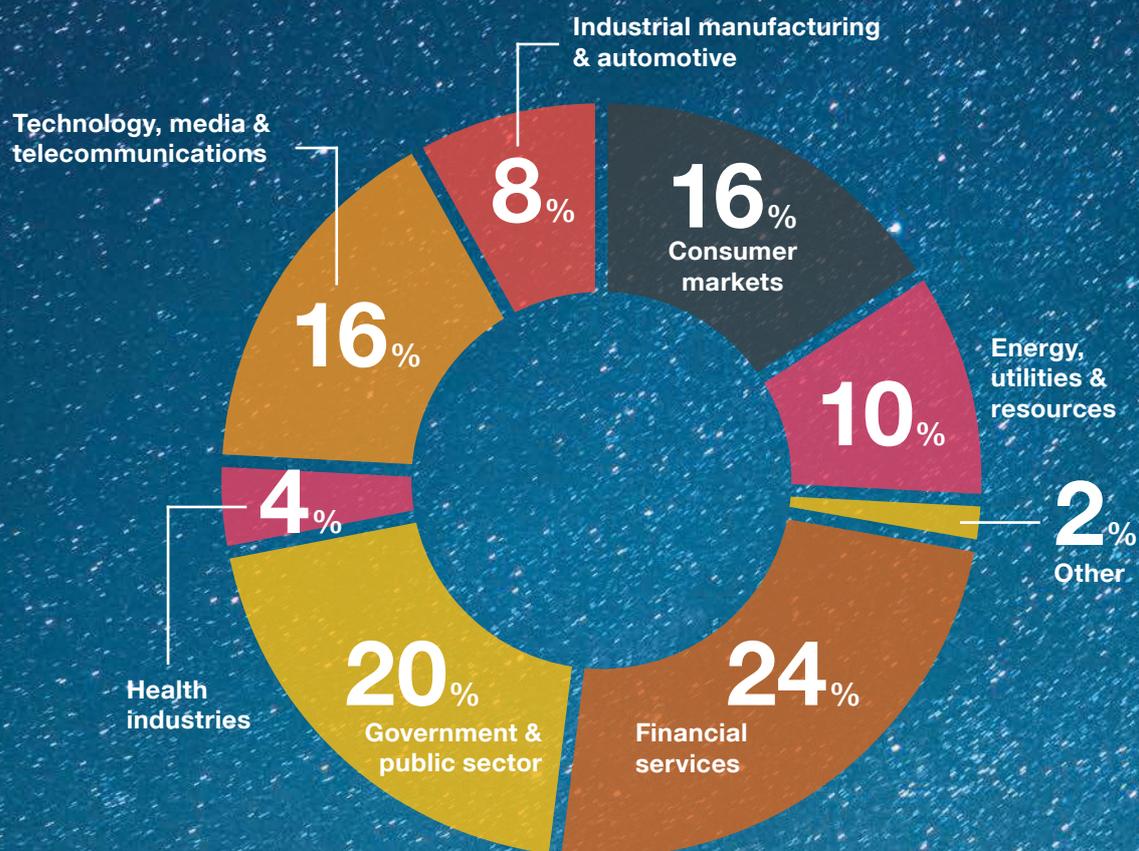
of respondents were C-suite

US\$1.7B

in losses



Industry sectors



Foreword



Trevor White

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



Economic crime, at **60%, is much lower than two years ago**, but instances of higher value fraud have increased considerably!

Chief Justice Mogoeng highlighted in an address at the University of KwaZulu-Natal in 2017 that private sector actors had escaped scrutiny in the past and while:

“There is a lot of wrongdoing, I dare say, in the public sector. A lot, as corruption and as mismanagement, but there is a lot of wrongdoing in the private sector. How it escapes the public space or find[s] some space there for a little while and immediately disappears, has confounded me for a very long time ...”¹

This has changed in the past couple of years with private sector frauds, due to the size of many of these and the involvement of senior management, now being much more widely reported on in the press and for much longer periods of time.

The results of our 2020 Global Economic Crime and Fraud Survey have turned up one major surprise, that being that the percentage of respondents who had experienced economic crime in South Africa declined for the first time in the last decade.

However, there was no surprise in the finding that bribery and corruption and financial statement fraud are still among the more prominent types of economic crime reported. This, combined with increased involvement of senior management in perpetrating such acts, has resulted in a sharp increase in the value of losses incurred as a result.

Our message is clear: To survive the catastrophic impact of economic crime, organisations need to be proactive, agile and resilient, to react in an appropriate manner and to do so swiftly. Organisations adopting the right approach to dealing with fraud will be able use these occurrences to emerge stronger.

Trevor White

¹ Steve Bhengu, “Mogoeng calls on SA to address corruption in the private sector.” East Coast Radio. 2017. <https://www.ecr.co.za/news/news/mogoeng-calls-sa-address-corruption-private-sector/> (accessed 5 February 2020)

Fraud perspectives: When less is actually more

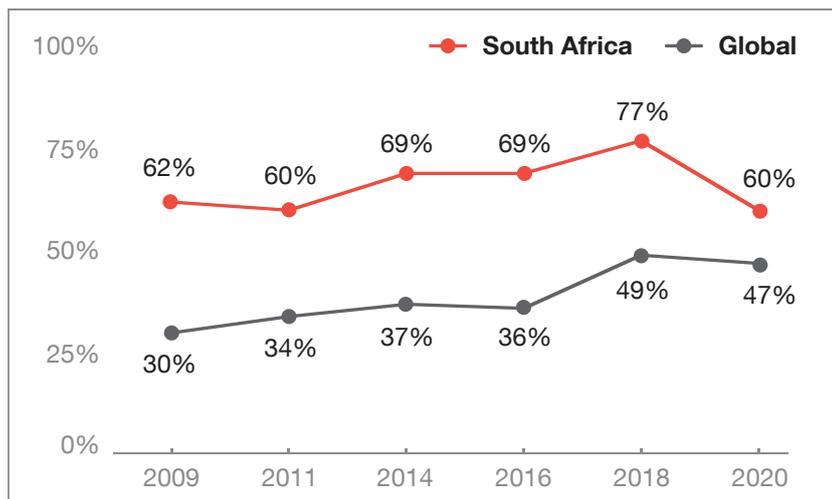


In this, the seventh edition of the PwC Global Economic Crime and Fraud Survey, we saw levels of fraud awareness and insight among South African organisations continue to outperform their global peers, with 73% of South African respondents indicating a high or extensive knowledge in this area, compared to 65% of global respondents.

Nevertheless, as witnessed by the major scandals that have rocked our local market over the past few years, the persistence of the scourge of economic crime is not to be ignored and awareness of the issues may serve us very little if action is not taken to actively eradicate the problem.

South Africa: Reported rate of economic crime

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



Source: PwC analysis

The silver lining of a very dark cloud: Reported rate of economic crime declines

As South Africans, we have become accustomed to being at the very top of the naughty list, but in the two years since our previous survey, we have seen a rather surprising drop in the reported rate of economic crime, from 77% in 2018 to 60% this year!

What could possibly have driven a 17 percentage point decline in the reported rate of economic crime? And should we be celebrating?

Having our reported rate of economic crime return to levels last seen in 2011, while global trends consistently exhibit higher levels than seen in the past 20 years, may offer a rare glimmer of hope for South Africa. But viewing this statistic in isolation presents a sadly distorted picture.

For one thing, at 60%, South Africa's rate of reported economic crime remains significantly higher than the global average rate of 47%. Added to this is the stark reality that the incidence of higher value serious economic crime has doubled in the past 24 months from 1% to 2%. There has also been a disturbing increase in the level of involvement of senior management as the main perpetrator, escalating from 20% in 2018 to 34% in 2020.

With respondents in India and China reporting the highest occurrence of economic crime, South Africa has slipped to third in the top ten ranking of countries with the highest reported economic crime in the world. Before now, India has never featured in the top ten.

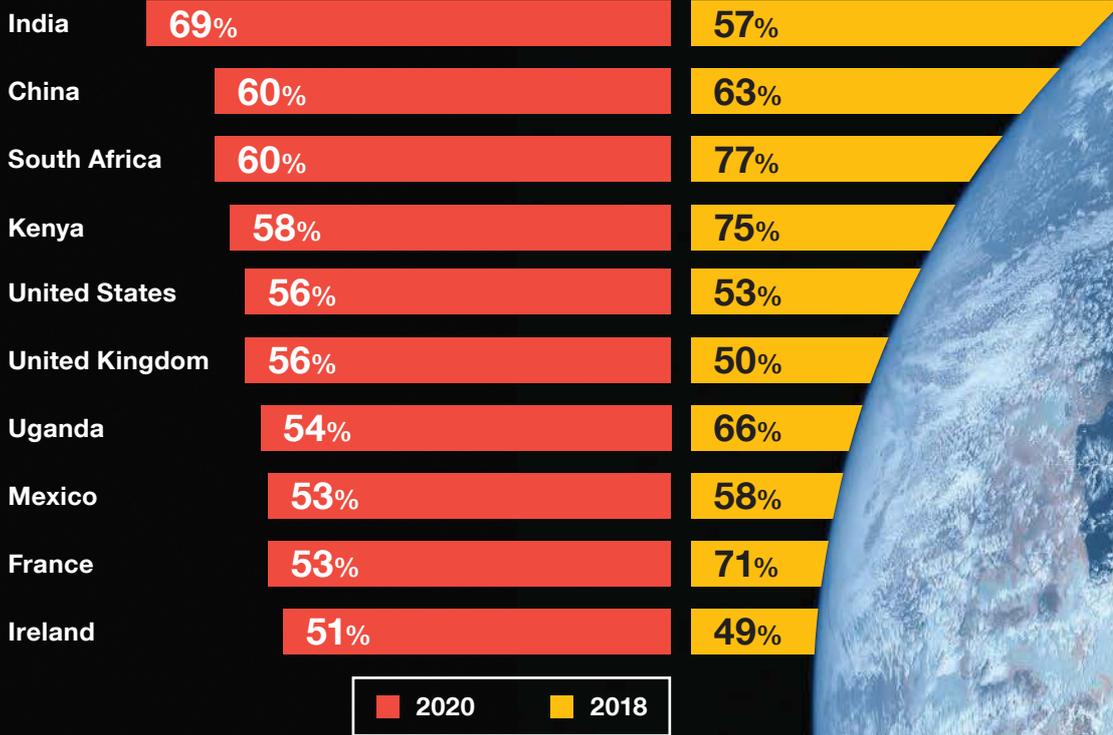


So very aware, yet
so very helpless:
How can we convert
knowledge to armour
in the fight against
economic crime?

Top 10 countries reporting most economic crime

Q

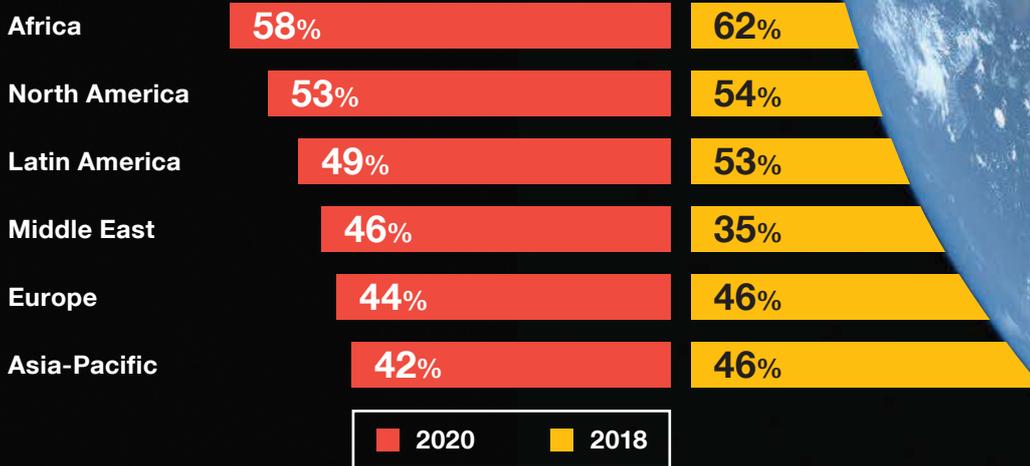
Has your organisation experienced any fraud and/or economic crime within the last 24 months?



Reported rate of economic crime by region

Q

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



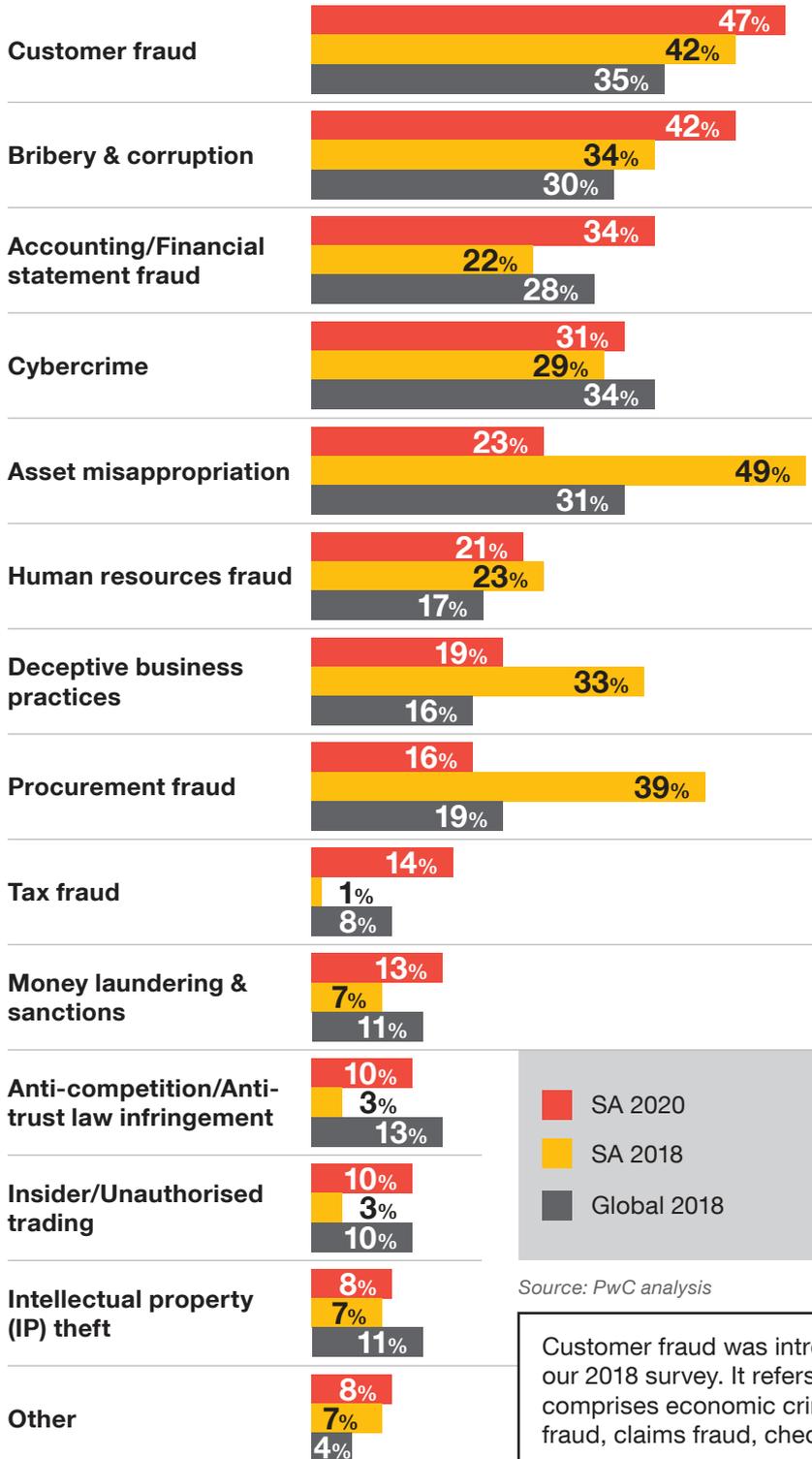
With 38% of global participants in PwC's 23rd Annual Global CEO Survey (2020) identifying China and India as the most important countries to their organisations overall growth prospects over the next 12 months (South Africa: 14%), this is a matter of serious concern.

China and India have emerged as economic powerhouses, but with fast-growing economies such as these being subject to concentrated attacks, the global impact is magnified. With the exception of the Middle East, which showed an increase in the regional rates of reported economic crime (by a significant 11 percentage points), all regions showed a decline. Africa still emerged as having the highest rate of economic crime, with the Americas following close behind.

Changing tides in the types of economic crime

Types of economic crime/fraud experienced

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



Source: PwC analysis

For the first time since this survey began, asset misappropriation was not identified as the most prevalent economic crime.

This year's survey ushers in a new era in which customer fraud has come to the fore as the most prominent economic crime, followed by bribery & corruption and financial statement fraud.

It is notable that while incidences of most fraud types declined in South Africa, occurrences of the top three rose, and so too did cybercrime, which seems to be creeping up to previous levels.

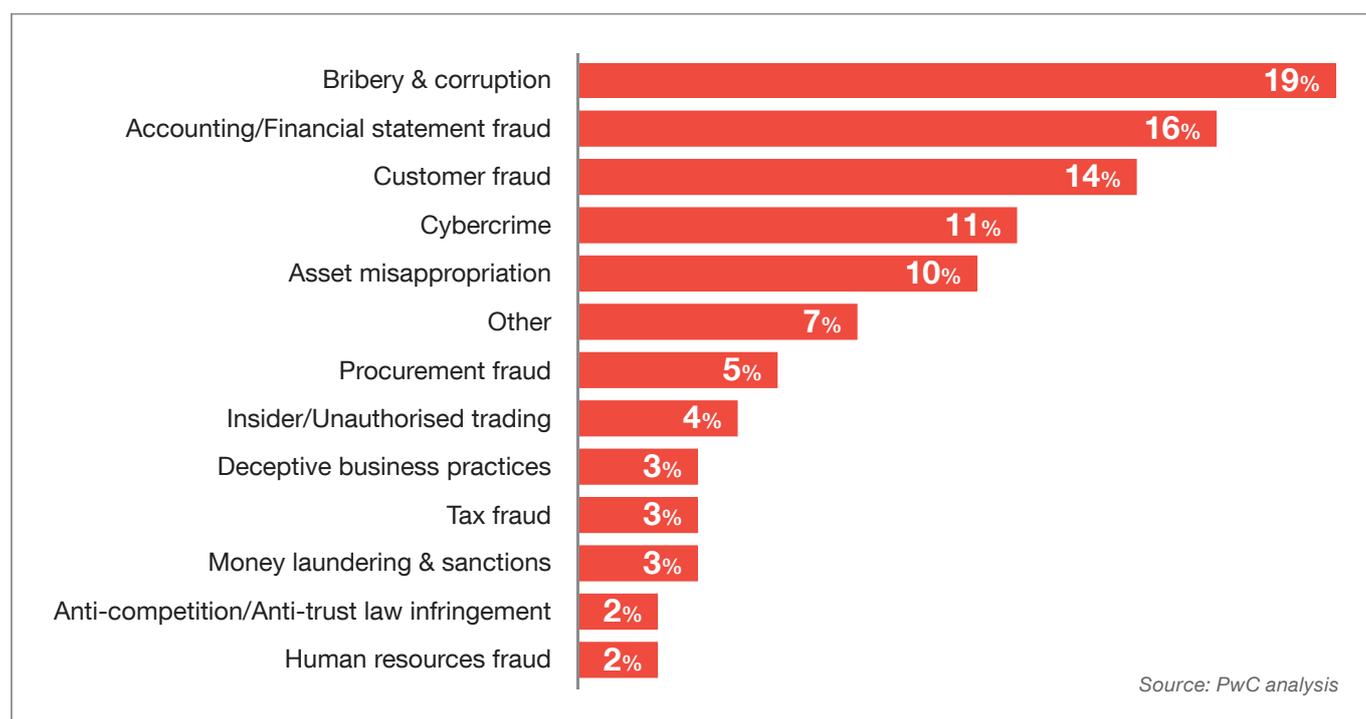
The significant increase in financial statement fraud is concerning as this type of fraud invariably involves senior management and the amounts are significant. The negative effect of this crime on all stakeholders and the future sustainability of the entity as a whole can be catastrophic.

Customer fraud was introduced as a category for the first time in our 2018 survey. It refers to fraud committed by the end-user and comprises economic crimes such as mortgage fraud, credit card fraud, claims fraud, cheque fraud, ID fraud and similar fraud types.



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)?



Given the recent scandals rocking South Africa, both in the public and private sectors, it comes as no surprise that a fifth of respondents consider bribery & corruption to be the most serious and disruptive economic crime to affect organisations.

The prominence of accounting and financial statement-related fraud, which has left many casualties in the past few years, has perhaps been one of the major factors prompting companies to take a cold, hard look at themselves and to honestly reflect on what is being done to counter the scourge of economic crime.

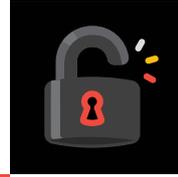
Cosmetic interventions are losing their lustre and trust is a precious commodity that is being lost. A third of South African respondents identified distrust as the most significant emotional impact brought about by acts of malfeasance.

The added risk, and a systemic risk at that, is that with the prominence of economic crime being perpetrated by so-called 'captains of industry', there is a tendency for common folk to rationalise criminal actions. The rise of customer fraud, which was only introduced as a category in the survey in 2018, is an indication of the erosion of the ethical fabric of our society.

When threats abound, both inside and outside the organisation, uncertainty regarding future prospects increases. This is reflected in our finding that 42% of South African respondents in PwC's 23rd Annual Global CEO Survey are not confident about their organisation's prospects for revenue growth over the next 12 months.²

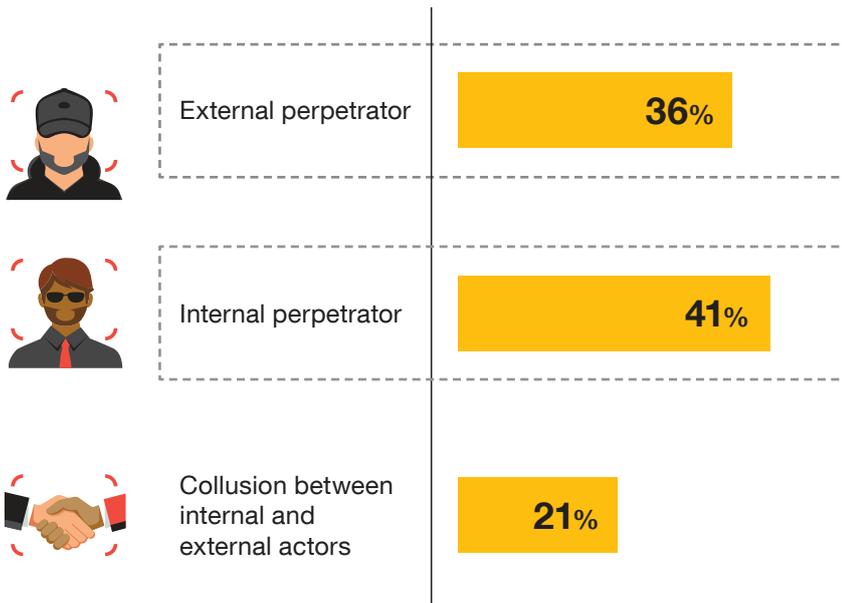
² PwC's 23rd Annual Global CEO Survey 2020 - www.ceosurvey.pwc

Redefining being bulletproof by looking inward



The actors that perpetrate economic crime in South Africa

Q Who was the main perpetrator of the most disruptive economic crime experienced?



Source: PwC analysis

Fraud hits companies from all angles and may take various forms, such as the internal perpetrator (41% of economic crimes were perpetrated by this group), the external perpetrator, and collusion between the two, which rears its head in one-fifth of cases, and is by far more difficult to detect and contain.

South African organisations have seen an upsurge in instances of senior management perpetrating fraud. Economic crimes perpetrated by senior management are often among the most sinister because of the ability (whether through delegated authority levels, system knowledge, or influence) of top executives to override (or conspire to override) internal controls.

With more than a third of South African respondents falling prey to this phenomenon, much greater focus on governance is required in organisations. The days of the passive non-executive board member have surely passed and there is a need for this independent oversight function to become more involved and ask the difficult questions, and thereafter demand and interrogate the answers provided.

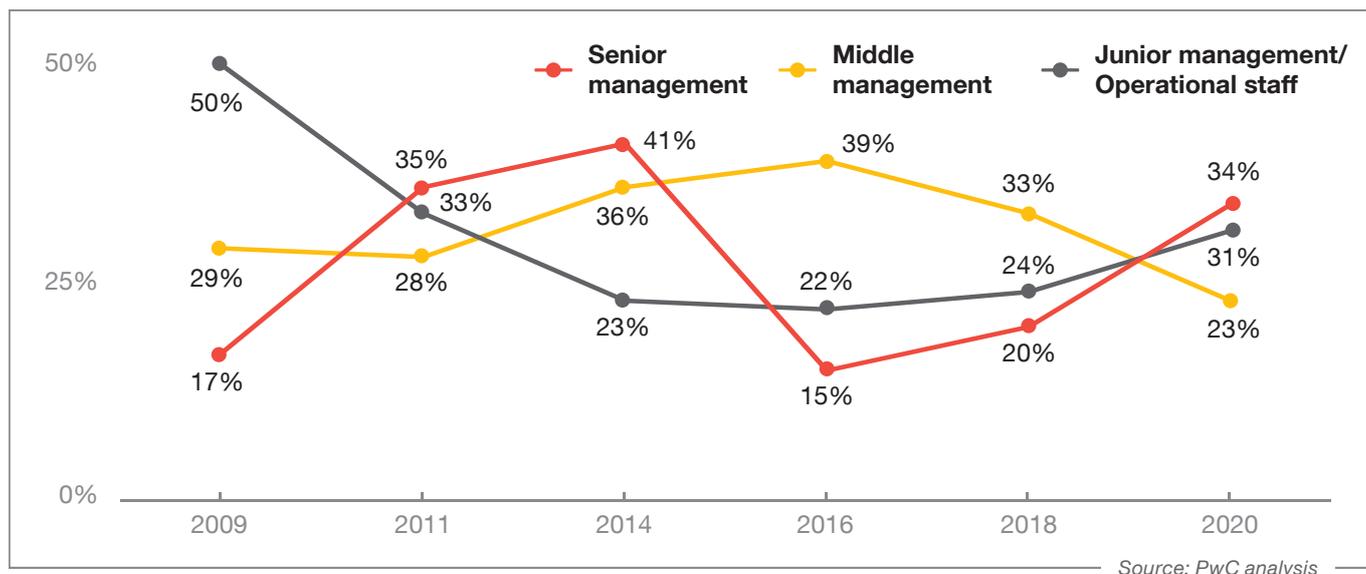


Recent experiences have woken us up to the fact that a major fraud risk area for organisations is the very custodians entrusted to run them.



Main perpetrators of internal fraud in South Africa

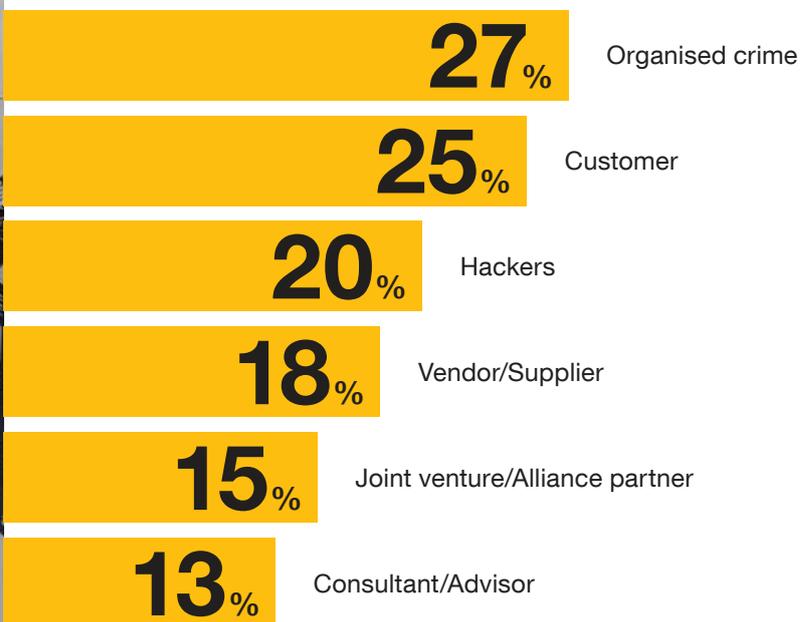
Q At what level within your organisation was the internal perpetrator of the most disruptive economic crime incident?



Look both ways: External forces remain a threat

External perpetrators of economic crime in South Africa

Q Who was/were the external perpetrator(s) of the most disruptive economic crime incident against your organisation?



Outsourcing has become the norm in companies and corporations seeking to minimize costs, but these cost-reduction exercises introduce a new dimension to the fraud landscape. Any chinks in the armour of these business partners become your risks and can lead to the unravelling of the most sophisticated fraud prevention strategies, if not formally and comprehensively addressed. It is telling, therefore, that three of the top five external perpetrators of economic crime qualify as business partners, in one form or another.

- One in five respondents cited vendors/suppliers as the source of their most disruptive external fraud;
- But more than half lack a mature third-party risk programme; and
- Almost a quarter of respondents (24%) have no third-party due diligence or monitoring programme at all.



In contrast to the trend globally, South African respondents cited organised crime as the highest rated source of external perpetrators with fraud committed by customers coming in a close second (at 25%) as the most disruptive fraud.

- From a global perspective, customer fraud is especially prominent in the financial services and consumer markets segments. This could be telling as industries shift to direct-to-consumer strategies.
- The good news? It's also one of the frauds where dedicated resources, robust processes and technology have proven effective in prevention.

One in five economic crimes perpetrated by external parties were committed by hackers, highlighting the fact that organisations cannot drop their guard in any area, especially if they are adopting greater levels of technological sophistication.

A close-up, high-resolution photograph of a person's eye, looking directly at the camera. The eye is light blue and has a sharp, focused expression. The skin around the eye is detailed, showing fine lines and texture. The background is dark and out of focus.

Businesses behaving badly

This year, for the first time, we asked respondents if their organisations had been accused of perpetrating a fraud. Of those who reported experiencing economic crime, nearly one in five South African respondents reported that their organisations had also been accused of committing a fraud, corruption, or other economic crime.

In almost equal numbers,

44% competitors

43% employees

31% customers (to a slightly lesser extent)

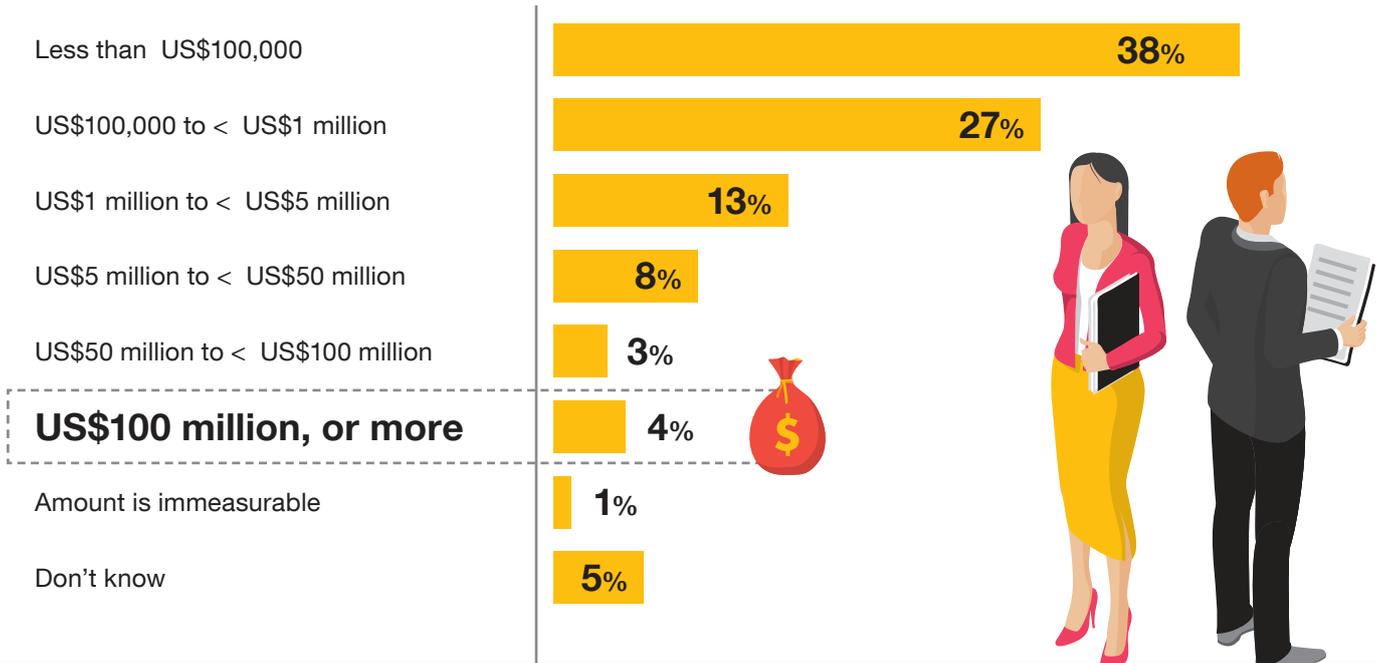
were most likely to point the finger. Only in a quarter of instances did a regulator make the accusation. This may speak to greater business and stakeholder activism, or perhaps that we have become a society that deflects attention away from our own actions by pointing at others.

Feeling the pinch: The cost of economic crime



Financial loss due to all economic crime experienced

Q In financial terms, approximately how much do you think your organisation may have directly lost through all incidents of fraud, corruption or other economic crime over the last 24 months?



The total losses associated with economic crime are difficult to calculate.

While some costs such as direct financial loss or costs due to fines, penalties, fraud response and remediation can be quantified, it is near impossible to place a value on other areas impacted by fraud — opportunity costs, reputational damage to a name or brand, loss of market position, and the impact on employee morale and productivity.

Threats arising from outside an organisation are generally transactional in nature, can potentially be monitored actively with relative ease and have limited (or at the very least, quantifiable) financial impact. Less predictable attacks such as bribery & corruption and internally-perpetrated fraud lend themselves to greater complexity because they attract more costly fines and bring with them other related issues (such as brand value impairment or lost revenue). These need to be managed and mitigated from the perspective of the amount of loss that could be sustained as a result of a decline in company or security value.

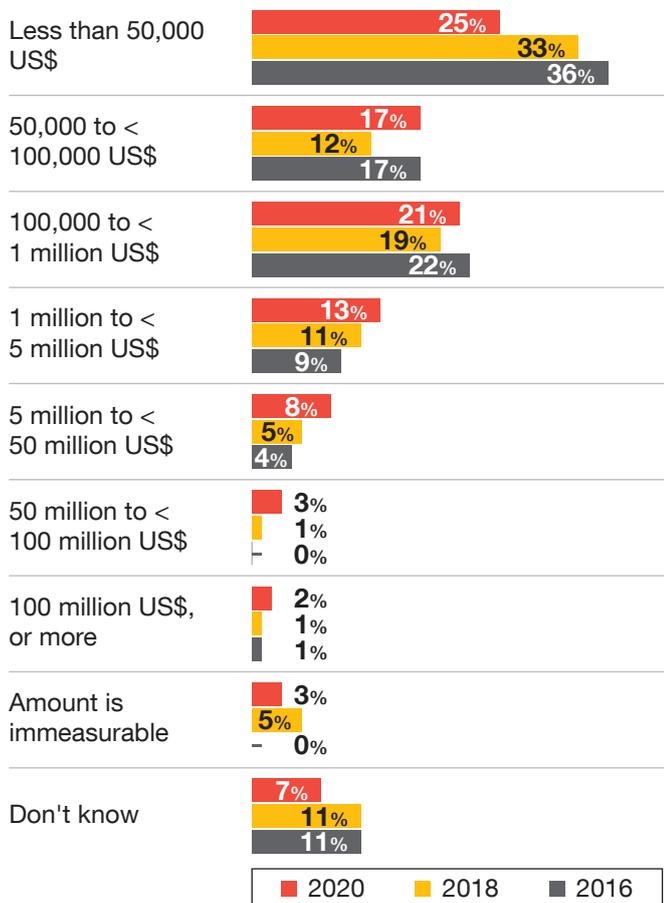
Roughly 7% of South African respondents who experienced a fraud in the last 24 months reported losing more than \$50 million across all incidents, with 4% reporting direct losses in excess of \$100 million for all incidents of fraud, corruption or economic crime experienced in the past 24 months. Incidences of losses in excess of \$100 million with respect to the most disruptive economic crime experienced by South African respondents doubled since the 2018 survey, from 1% to 2%.



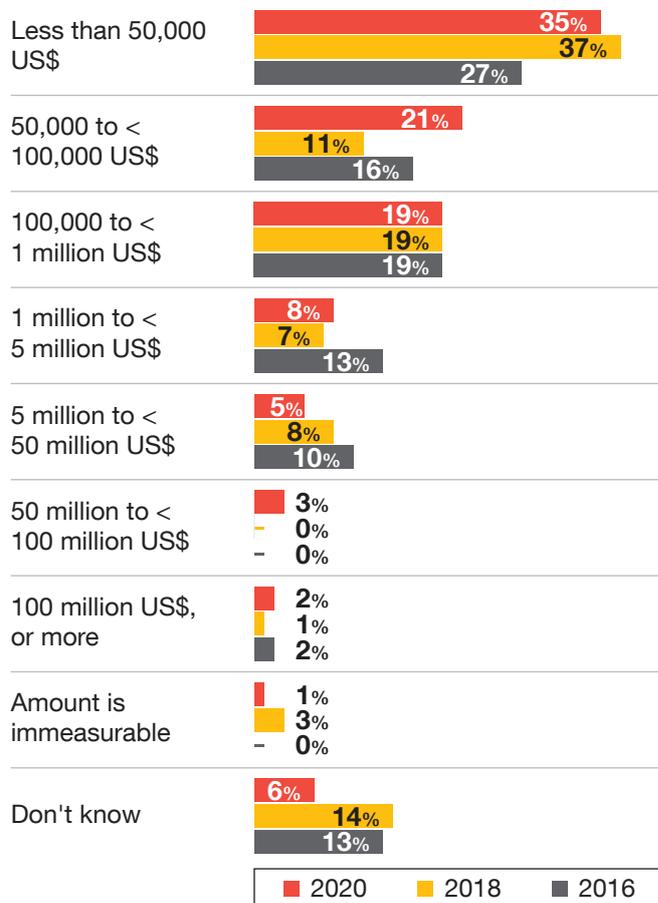
Financial loss associated with the most disruptive economic crime experienced

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

Global



South Africa



Source: PwC analysis

Endemic corruption

One in five South African respondents cited bribery & corruption as the economic crime which had the most disruptive impact — and almost half the companies surveyed were themselves accused of bribery & corruption. This remains a big challenge to business and government alike.

In the past 24 months, 42% of South African respondents (global: 29%) say they have been asked to pay a bribe in the course of doing business. Add this to the 44% who believe they have lost an opportunity to a competitor who paid a bribe, and you realise how dismal the situation is.

Considering the increased reported prevalence of these kind of incidents since our 2018 survey, swift and decisive action needs to be taken.

A wake-up call for boards and regulators



As businesses have evolved from sole traders to the complex organisations of today, so too have the structures governing them. These include the board of directors and various regulators, whose primary responsibility is independent oversight of what is happening at the organisation.

Changes to board structures have been spearheaded by the various King Codes, among other regulations. However, recent corporate failures in South Africa and abroad highlight the fact that despite these structures and oversight, corporate failures as a result of economic crime continue to occur.

Regulators are actively looking at these events to determine what went wrong and how they can be prevented in the future. This is likely to lead to a new wave of additional regulatory oversight, despite the fact that 53% of South African participants (global: 36%) in our 23rd Annual Global CEO Survey are 'extremely concerned' about the threat of over-regulation to their organisations' growth prospects.

In an environment of pervasive fraud and growing scrutiny from regulators and the public, no organisation can afford blind spots. Our survey uncovered two particular anomalies and disconnects that call into question current anti-fraud strategies:



Allegations and irregularities should be investigated

It seems self-evident, but the best way to avoid getting embroiled in another fraud is to investigate the last one and to take appropriate remedial action. However, **42%** of South African organisations (global: 44%) did not conduct an investigation after finding fraud.



Incidents should be taken seriously and reported appropriately

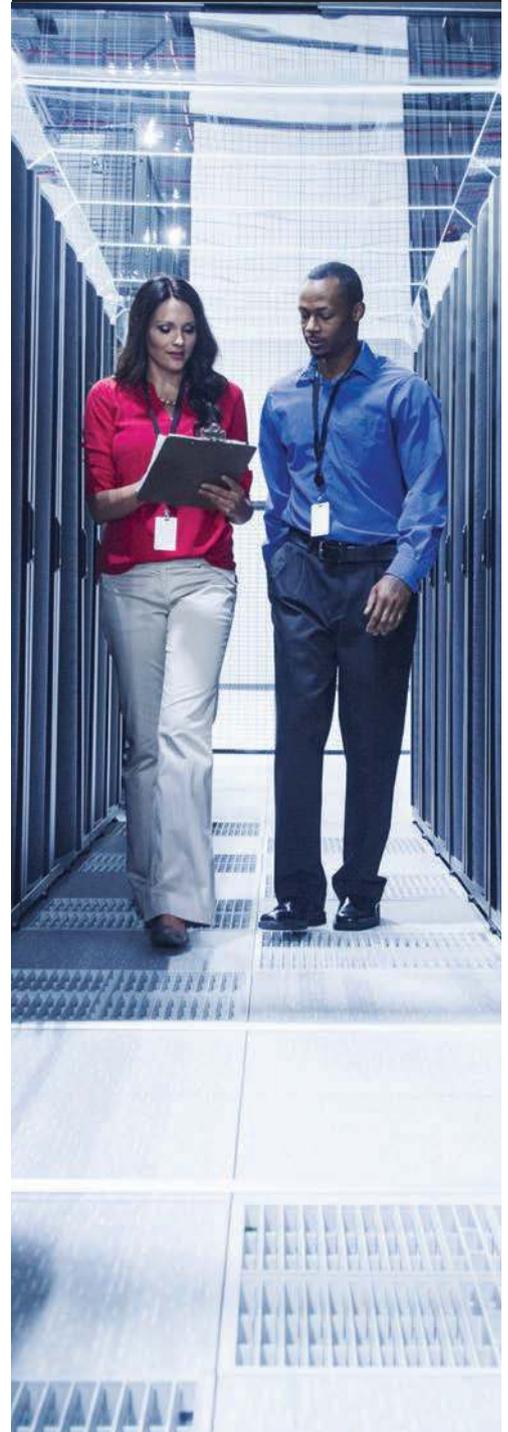
Our survey uncovered some shocking findings:

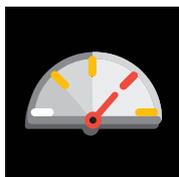
72% (global: 73%) of incidents were not disclosed to the auditors

66% (global: 69%) of incidents were not disclosed to regulators or law enforcement

59% (global: 65%) of incidents were not disclosed to the board of directors

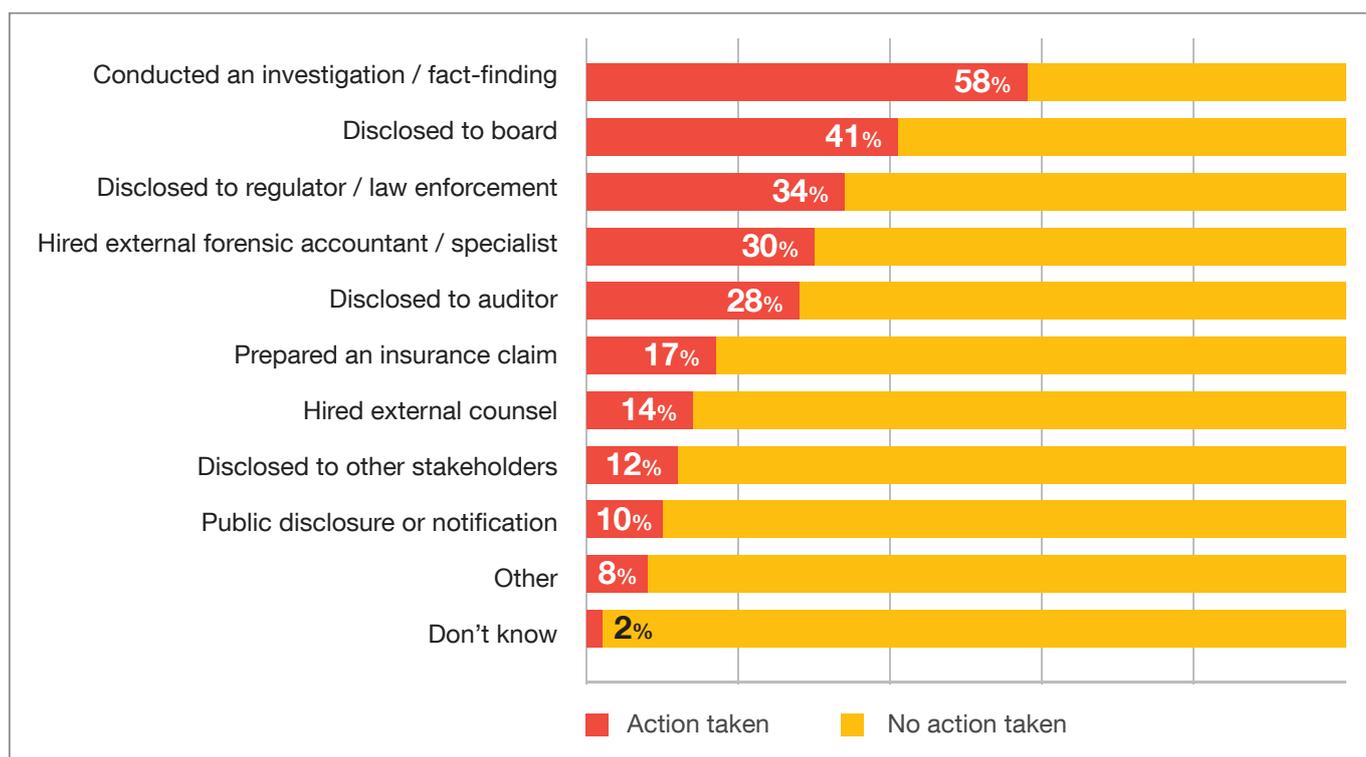
Are you assessing the threats you face well enough, or are gaps in your perception leaving you dangerously exposed?





Responses to incidents of economic crime

Q How did your organisation respond to the incident?



Source: PwC analysis

In our 2018 survey, we reported that one of the best antidotes to perpetrators rationalising their fraud is transparency and openness. If the organisation is not investigating and/or not reporting its findings it has a long way to go in remedying the problem.

In addition to the non-reporting highlighted in our survey, our experience confirms that reporting to the board and other oversight bodies often falls short of what is required for them to perform their oversight roles.

Poor reporting is often as a result of:

- Defensive/Excessive reporting — resulting in an overwhelming amount of information;
- Oversimplified/Underplayed reporting — resulting in insufficient information to understand the extent of the incident; or
- Deceptive reporting — resulting in a perception that the relevant information is being reported, when in fact it is withheld or buried intentionally.

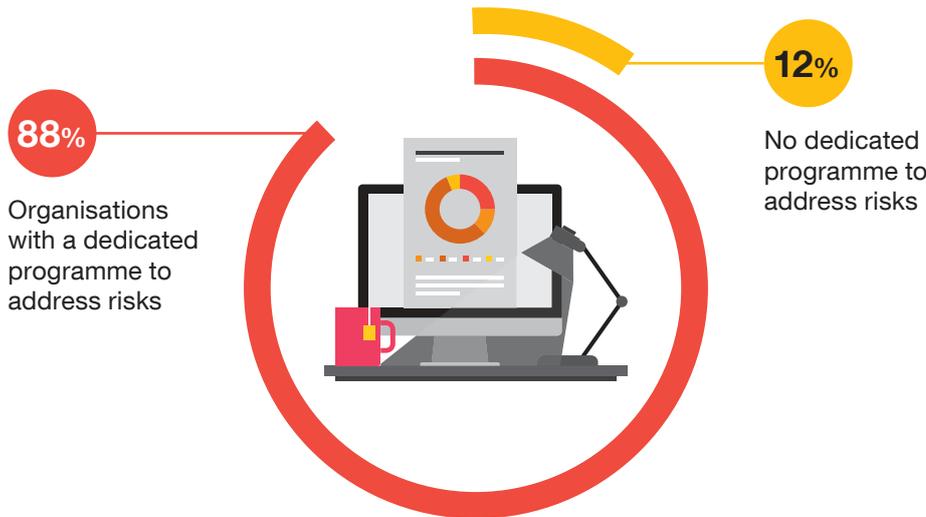
These poor reporting strategies either leave the recipients unable to determine what to do with the information or without the information necessary to perform the necessary oversight.

Two questions we should all be asking are:

- Are organisations as mature as we think?
- Are there heightened risks that require additional oversight by those charged with governance?

Are organisations as mature as we think?

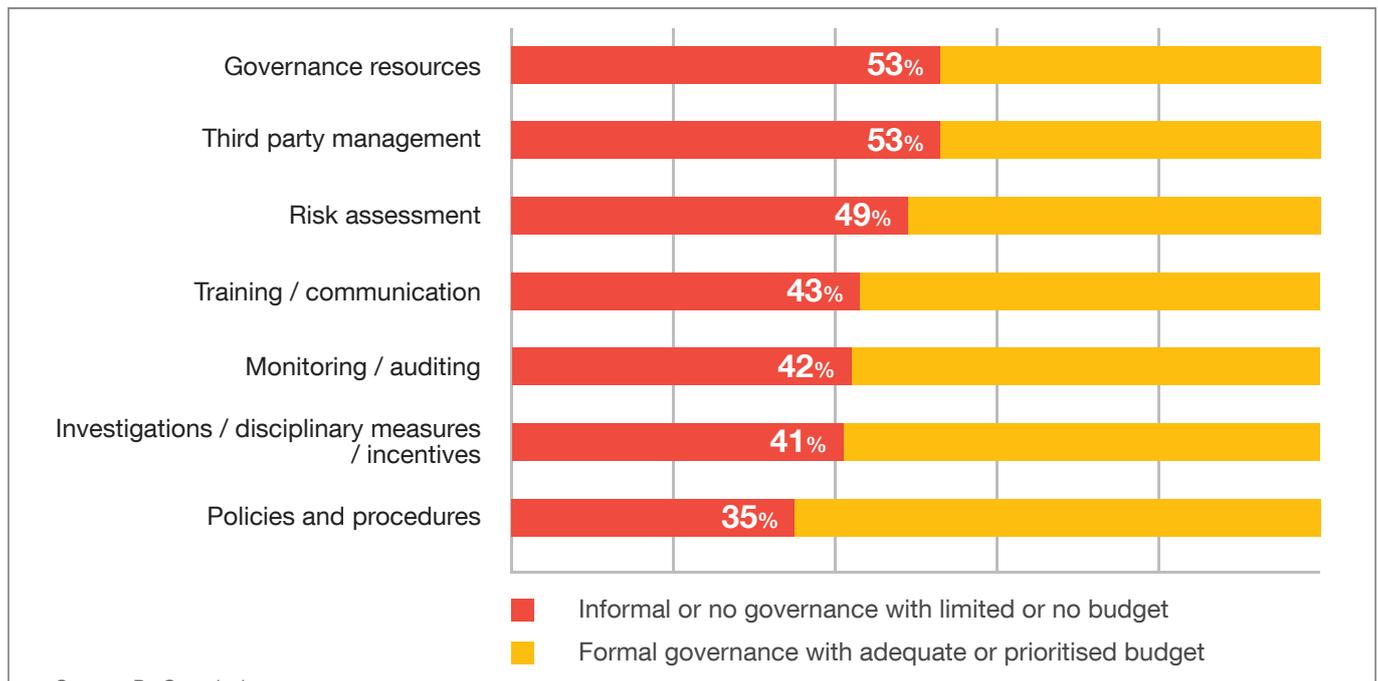
Q Which option best describes the key elements of your overall fraud programmes in relation to governance/resources?



Our findings reveal that a significant percentage of organisations are not disclosing incidents to their board and regulators, despite the fact that 88% of South African respondents say they have some form of dedicated anti-fraud programme.

Formalised vs unformalised governance programmes

Q Which option best describes the key elements of your overall fraud programmes?



Source: PwC analysis

Our survey reveals that, on average, only 55% of South African organisations have formal governance over anti-fraud programmes. With only half of organisations reporting formal governance over their fraud risk assessments, and fewer than that over fraud resources and governance, the question arises whether boards of directors should be more involved.



Heightened risks that require additional governance

Ten red flags seen in recent governance failures

1

Dominant CEO

- Belittles members of the board and others who disagree
- Runs organisation through fear
- Often pride-driven and egocentric
- Will create a team around them who will not rock the boat by asking questions

5

Expertise of board is out of sync

- Directors are vastly experienced, but are only passengers and do not contribute
- Directors are vastly experienced, but in different industries and cannot contribute effectively
- Directors do not understand the operating environment and business model complexity of the organisation

2

Unhealthy board dynamics

- The chair uses a 'tick-box' method to move through the agenda
- Members reluctant to express their points of view in front of management
- Some directors have significant influence on board decisions

6

Watch the hidden tactics to hide fraud

- Material year-end transactions are performed and approved, without commercial substance, just before financial statements finalisation
- Related parties are not adequately identified

3

Inconsistent governance and reporting standards

- Policies, standards and frameworks are not complied with and not questioned by the board
- Multiple auditors in the group, making it difficult to see the full picture

7

Culture of deference and lack of challenge

- Members are not willing to put their hands up and ask the challenging or 'stupid' questions
- Do not ask questions when company is healthy – even if industry is not performing well
- Directors do not get proper answers to their questions and don't probe further

4

Monitoring of management relations and performance

- Management's personal wealth, including incentive/performance bonuses, is linked too closely to the performance of the company
- Inappropriate close relations between the CEO and CFO

8

Ineffective nominations committee

- Composition and expertise of the board is of no importance
- Role of the nominations committee to ensure board is balanced and equipped to perform its required duties is undermined

9

Weak assurance functions

- Weak assurance functions led by inexperienced CAE, CRO or CCO
- Not focused on strategic business risks
- Does not have the required standing

10

Board pack not fit for purpose

- Packs are excessively congested and filled with information of poor quality or little importance to board members — used to mask important and/or incriminating information
- Not enough time to prepare because board packs arrive late

These dynamics bring up the need to ‘trust, but verify’.

While two-thirds of organisations surveyed are covering the basics — policies, procedures, training and monitoring — barely half are dedicating resources to risk assessment and governance. These are, or should be, the head, heart and engine of a robust and credible anti-fraud programme — and some regulators are beginning to demand more than "check-the-box" compliance, which can only be achieved with the necessary resources and oversight.





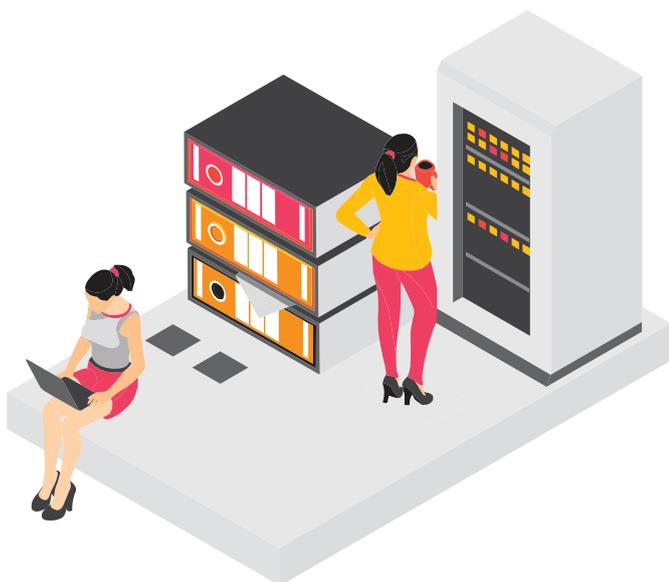
Fraud insights:

Prepare.
Respond.
Emerge stronger.

6

Taking initiative: Preparing for fraud

From a global perspective, on average, companies have four dedicated programmes in place to mitigate fraud risk (larger companies with more than 10,000 employees average more). While almost sixty percent of South African respondents say they have policies and procedures in place that include training and monitoring, only around half of organisations in South Africa are dedicating resources to risk assessment, governance, and third-party management.



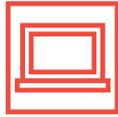
What measures are you taking to prevent fraud? Can you adequately identify fraud in your environment? Have you considered what is working — and what simply isn't? Do your programmes, methods and technology close off all gaps or are there gaping holes in your armour? What improvements can be made right now and how are you managing these?

So how do we solve for this serious issue?



An active and robust risk assessment process

Companies should perform robust risk assessments, gathering internal input from stakeholders across the organisation and across geographies, to identify risks and assess mitigating factors. External factors should also be considered during risk assessments as ignoring the wealth of information available in the public domain could leave potential gaps, leaving your organization exposed. This should not be viewed as a once-off exercise and a programme should be instituted where risks are assessed at regular intervals.



Technology alone is not enough

Supplement your tech with the right governance structures, relevant expertise, and robust monitoring

No single solution or tool can be regarded as invincible or sufficient — economic crime evolves far too quickly and your arsenal needs to follow suit. Organisations must embrace the idea that there is no quick, single-solution way to solve the ‘fraud problem’. Technology alone will not protect you — like any piece of machinery, it is imperative that these tools are driven by resources with the right expertise that are appropriately placed within the structure of an organisation. A dedicated, regular monitoring programme also needs to be instituted to keep technology current, working and effective.



Eyes wide open to what's going on

Rapid reaction time and the ability to act swiftly and mobilise the right people, the right processes and the right technology as and when a fraud incidence occurs, are essential elements of an effective fraud risk programme. Ideally, organisations should be securing the perimeter to ensure that, to the extent possible, no infiltrations take place. The programme must also recognise that evolution is inevitable, and intrusions will occur — it's how quickly an organisation can adapt to the attack that will determine how risks are addressed and damages or losses are contained.

Technology: Just one piece of the puzzle

Many organisations have invested heavily in new tools and techniques in recent years. However, many survey participants shared reservations about deploying technology:

- Forty percent of South African respondents ‘strongly agree’ that they’ve been able to implement or upgrade their technology. However, costs, limited access to resources, and lack of proper systems are among a number of the obstacles encountered.
- Of those who aren’t implementing new anti-fraud technologies, nearly one in three say it’s because they struggle to see its value.
- Considering alternative/disruptive technologies and techniques emerging, almost

30%

of South African participants (global: 26%) say they are using artificial intelligence (AI) and most see it as a valuable tool in the fight against fraud.



Fraud insights:

Prepare.
Respond.
Emerge stronger.

7

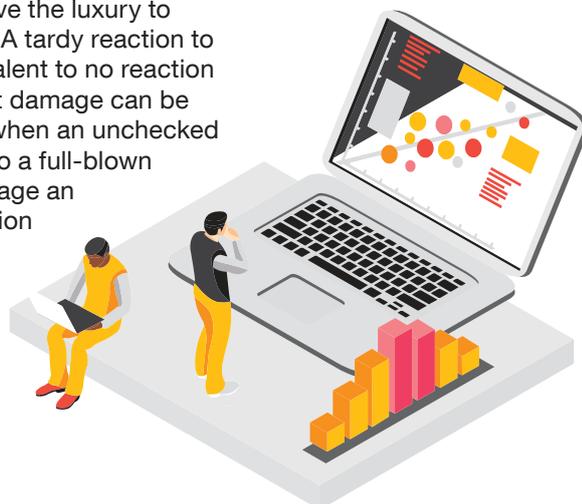
When the time comes, react the right way



How an organisation responds to fraud when it occurs can determine whether it perishes, survives or thrives as a company. Sixty percent of South African survey participants that experienced and addressed a disruptive fraud incident believe that they ended up in a better place after the investigation. Forty-two percent of respondents didn't conduct an investigation at all and more than half the incidents were not disclosed to the board. What is equally concerning is that board members never asked these questions! Since fraud is so prevalent in South Africa, this may be seen as an indictment of the way in which some boards execute their duties, and calls into question whether they are acting in the best interests of their shareholders.

Organisations and the structures that govern them are expected to do more, not only by regulators, but also by the broader investment and stakeholder communities.

Companies do not have the luxury to react in a lax manner. A tardy reaction to a fraud event is equivalent to no reaction at all and the resultant damage can be immense, especially when an unchecked situation escalates into a full-blown crisis, which can damage an organisation's reputation and value.



Only **58%** of South African respondents (global: 56%) conducted an investigation of their most serious fraud incident. In almost sixty percent of cases, the incident was not disclosed to the board at all.

Conduct an investigation

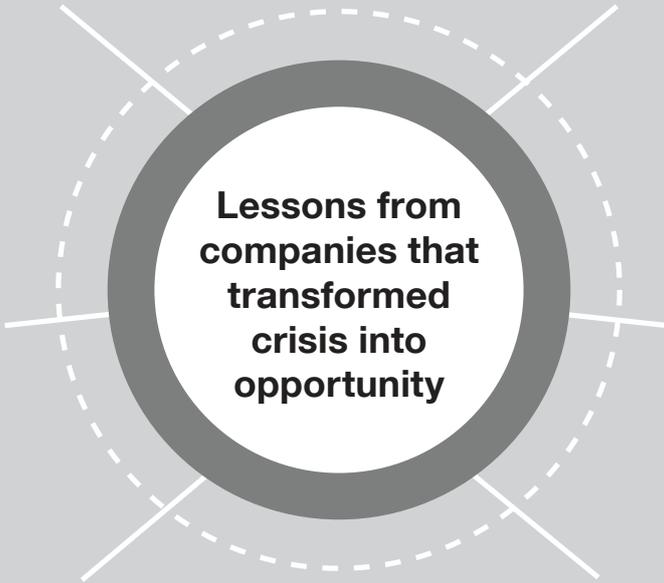
Getting to the root of the problem and understanding the issue, and perpetrators, is key to preventing further and future fraud. An honest look at your capability and objectivity is crucial at this point and it may be in the best interests of an organisation to seek external assistance to investigate fraud, especially if the required skills are not available internally or if resources are scarce.

Disclose the incident to government authorities and/or regulators

Disclosing the fraud early can sometimes result in a more favourable outcome with regulators and authorities. In contrast, not doing so could become an existential threat to an organisation.

Disclose the incident to the board of directors

Playing open cards with the governance structures serves to enhance the role of these structures and contributes to the ongoing development and improvement of an organisation. This serves to activate board members to truly fulfilling their roles, rather than being passive occupiers of boardrooms.



Lessons from companies that transformed crisis into opportunity

Bolster internal controls, policies and procedures

While some policies and procedures may be easy targets, it's important to assess operations locally, regionally and globally to identify gaps and areas requiring enhancement.

Take disciplinary action against employees

In line with regulatory guidance, compliance programmes should apply universally and no one should be beyond their reach. Furthermore, no person should be deemed too valuable to be disciplined. Consistent enforcement of a compliance programme is one of the keys to its effectiveness.

Conduct training

Training not only better informs staff of new policies and procedures, it also promotes a stronger culture around fighting fraud. Getting personnel to take ownership of their custodial duties can easily be achieved through making them part of the solution.





Fraud insights:

Prepare.
Respond.
Emerge stronger.

8



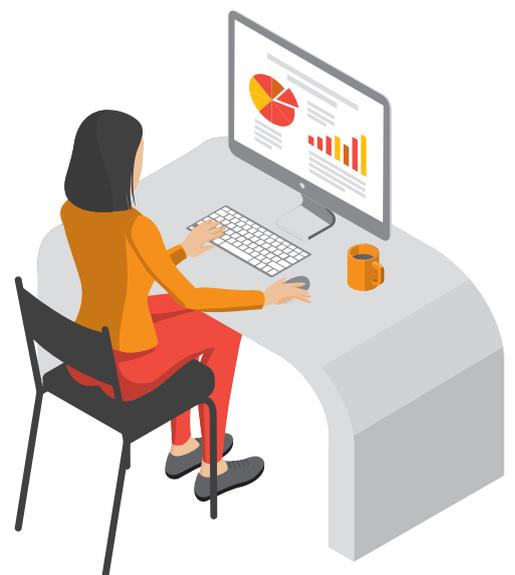
Rising from the ashes: Measuring success

Fraud departments within organisations are often battling to get out of the catch-up zone, constantly needing additional budget in order to better equip themselves to counter the seemingly unrelenting, and very innovative challenge that is economic crime. New technologies to invest in, new programmes to implement, or additional personnel and resources to employ costs money, lots of it.

Almost half of South African respondents are planning to increase their spend on fraud prevention in the next two years. A question that this raises is whether these initiatives are working and whether the investments made are bearing fruit. How should organisations go about measuring this? Is there a realistic yardstick to measure success in this arena, or are investment committees expected to blindly pump funding into what they see as an abyss?

It is difficult to quantify the benefits of a fraud-fighting tool, just as it is near impossible to fully quantify the cost of fraud and the impact it has on an organisation. What we do know is that fraud events and fraudsters that are left to run rampant cause more damage and result in higher losses to organisations than those that are slowed down or stopped in their tracks by active fraud prevention initiatives and investments.

Companies with dedicated fraud programmes in place generally spend less (relative to revenue) on response, remediation, and fines.



While having a fraud programme may be necessary, it will invariably not be sufficient without being actively adapted by means of periodic assessments and refinement, regular testing and revisiting.

There are a number of reasons for this:



Business models frequently evolve before risk programmes are established, leaving companies exposed to unexpected risks. For example, this might involve the simple introduction of a business partner, a change that could leave an organisation exposed if proper measures, due diligence and risk impact assessments are not considered.



New technology creates new ways of doing business. For instance, we see an increasing level of convergence in certain industries, such as technology companies offering financial services, or health companies entering consumer markets. With such changes to the business environment, risk management programmes must be agile and adapt in order to remain relevant and take on new and evolving risks as they emerge.



A hotline call or audit finding may yield a risk previously not considered.

Regulators are also an important factor to consider. As complexity grows in the business environment, so too does the sophistication of the schemes aimed at breaking the system. Laws and regulations need to keep up with these waves of innovation.

Many recognise that compliance programmes should be risk-based and right-sized, and that no programme is guaranteed to catch all improper activities. There is no one-size-fits-all approach to compliance, and a programme at a large telecommunications company should look quite different to one at a small retailer. However, both must be adequate in addressing the particular risks each organisation faces.

So too, there is no single method for assessing the effectiveness of a fraud programme or the initiatives that have been put in place.

How and where do you begin? A natural starting point is to understand what can and cannot be quantified and start collecting the necessary data. For external parties, consider including such metrics as vendor rationalisation statistics, vendor rejection statistics, participation of vendors in training programmes, vendor certifications, or reductions in findings during third-party audits.

The key to success is having a defensible measurement in place that will help to demonstrate that the programme area has been tested as well as how it will practically prevent or detect problematic misconduct in the future.





Conclusion: The writing is on the wall

So where do you stand? How do you fare when it comes to preventing, detecting and responding to economic crime? Can you proclaim to be ‘bulletproof’ or do you have chinks in your armour?

Sitting on the side-lines is not an option — decisive action is paramount to ensuring your organisation is protected, at least to the extent possible at any given time. What this equates to is an urgent need for a diligent programme of revisiting and refining your defences regularly, actively and realistically. Don’t find yourself on the wrong side of the evolution of economic crime and criminals — their methods change with frightening speed, and so too must your protection against attacks.

The challenge is daunting, but the alternative is terrifying — gaps in your defences and wilful blindness to weaknesses in your protection are open invitations to disaster, and based on the increasing losses we are seeing, these may even lead to your organisation’s demise.

No business can claim to be immune to the scourge of economic crime and fraud, so rather than waiting for an incident to lay siege, take a proactive stance and increase your levels of insight and awareness — including increasing awareness from a board oversight perspective as well.

Proactivity, agility and resilience are key ingredients in the fight against economic crime, and your ability to emerge stronger will depend on your organisation’s response to incidents, before, during and after they occur.

Contacts



PwC Southern Africa Forensic Services Leader

Trevor Hills

Partner, Johannesburg
+27 (0) 11 797 5526
trevor.hills@pwc.com

Anti-bribery & Corruption

Trevor Hills

Partner, Johannesburg
+27 (0) 11 797 5526
trevor.hills@pwc.com

Cybercrime & Forensic Technology Services

Junaid Amra

Partner, Durban
+27 (0) 31 271 2302
junaid.amra@pwc.com

Dispute Resolution & Litigation Support

Trevor White

Partner, Johannesburg
+27 (0) 31 271 2020
trevor.white@pwc.com

Greg Truter

Partner, Johannesburg
+27 (0) 11 797 4661
greg.truter@pwc.com

Malcolm Campbell

Partner, Cape Town
+27 (0) 21 529 2676
malcolm.campbell@pwc.com

Expert Accounting

Greg Truter

Partner, Johannesburg
+27 (0) 11 797 4661
greg.truter@pwc.com

Financial Crime & Compliance

Kerin Wood

Associate Director, Johannesburg
+27 (0) 11 797 5246
kerin.wood@pwc.com

Fraud Prevention & Consulting

Boitumelo Lekoko

Partner, Johannesburg
+27 (0) 11 287 0163
boitumelo.lekoko@pwc.com

Global Intelligence

Chesirè le Roux

Associate Director, Cape Town
+27 (0) 21 529 2326
chesire.le.roux@pwc.com

Forensic Investigations

Malcolm Campbell

Partner, Cape Town
+27 (0) 21 529 2676
malcolm.campbell@pwc.com

Gerhard Geldenhuys

Partner, Bloemfontein
+27 (0) 51 503 4106
gerhard.geldenhuys@pwc.com

Trevor Hills

Partner, Johannesburg
+27 (0) 11 797 5526
trevor.hills@pwc.com

Boitumelo Lekoko

Partner, Johannesburg
+27 (0) 11 287 0163
boitumelo.lekoko@pwc.com

Itumeleng Serithi

Partner, Johannesburg
+27 (0) 11 797 7445
iserithi@pwc.com

Greg Truter

Partner, Johannesburg
+27 (0) 11 797 4661
greg.truter@pwc.com

Lionel van Tonder

Partner, Johannesburg
+27 (0) 11 287 0152
lionel.tonder@pwc.com

Trevor White

Partner, Johannesburg
+27 (0) 31 271 2020
trevor.white@pwc.com

Moazam Fakey

Associate Director, Johannesburg
+27 (0) 11 797 4750
moazam.fakey@pwc.com

Gerard Sutton

Associate Director, Port Elizabeth
+27 (0) 41 391 442
gerard.sutton@pwc.com



© 2020 PwC. All rights reserved.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

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, PwC does 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.

© 2020 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity.

Please see www.pwc.com/structure for further details

(20-25093)