Economic Crime: A South African pandemic

No sector or region is immune

69%

More than two in three organisations report being victims of economic crime

32%

Almost a third of organisations have experienced cybercrime, and this figure is growing rapidly

70%

Almost three quarters of respondents view local law enforcement as inadequately resourced to fight economic crime, leaving the onus to do so on organisations

pwc

Leading observations

1 *Economic crime is a serious threat in SA*

- More than two thirds of South African organisations (69%) have experienced economic crime
- Detection methods are not keeping pace
- Significant change in the profile of perpetrators, with external and internal actors now evenly split

What opportunities are available for countering economic crime proactively?

Economic crime rates remain unacceptably high

2 *South Africans exhibited low levels of confidence in local law enforcement agencies*

- Economic crime is costing businesses billions
- 70% of South African respondents view local law enforcement agencies as being inadequately resourced and trained
- Poor perception of law enforcement is also a problem in many first-world countries

What action do you take once a fraud has been detected?

Local law enforcement agencies are seen as being inadequately resourced and trained

3 *Cybercrime is a threat to all aspects of business*

- 32% of South African organisations reported having been victims of cybercrime (same as the global average)
- Most organisations are still not adequately prepared for, or even understand the risks they face – only 35% of organisations have a cyber incident response plan
- Engagement of leadership is critical, but only 48% of board members request information about their organisation's state of cyber-readiness

How will your cyber response plan stand up to reality?

Cybercrime rises to fourth most reported type of economic crime (up two places from 2014)

4 *Bribery and corruption continue to evolve*

- 15% of SA organisations have been asked to pay a bribe
- While 88% of SA organisations have a code of conduct in place, only 58% say that training is provided regularly
- More than half of SA respondents believe it is 'likely' they will experience bribery and corruption in the next two years

Is your compliance programme properly addressing the evolving risk landscape?

We cannot afford for corruption to become an accepted way of life in South Africa

5 *Poor data quality and skills shortages are undermining the efficacy of anti-money laundering systems*

- Only 50% of money laundering and terrorist-financing incidents in financial services organisations were detected by system alerts
- One in three SA organisations experiences difficulty in sourcing personnel with skills in the areas of anti-money laundering/combating the financing of terrorism
- More than a third of financial services respondents that have undergone inspections by regulators had to address major findings

How would newer technology and data analytics transform your monitoring capabilities?

The cost of compliance (and non-compliance) continues to rise

Contents

Foreword

It will surprise few to learn that economic crime such as asset misappropriation, procurement fraud, corruption, cybercrime and human resources fraud continues to be a major concern for organisations of all sizes and in virtually every sector.

But the real story is not so much that economic crime stubbornly persists. Rather, it is that economic crime is threatening your business processes, eroding the integrity of your employees and tarnishing your reputation – which is why this year's report is focused on how and where it may be affecting you. Armed with this knowledge, you'll be able to better address the issue from both a preventive and a strategic perspective.

The threats from economic crime continue to evolve. Like a virus, economic crime adapts to the trends that affect all organisations. An especially impactful megatrend includes the increasing reliance on technology and technology-enabled processes in all aspects of business.

With organisations increasingly depending on technology, it's perhaps not surprising to find that cybercrime continues to increase in volume, frequency and sophistication. A third of all respondents report having been victimised by cybercrime. Meanwhile, sometimes overlooked categories of economic crime such as procurement fraud and human resources fraud are, together with bribery and corruption, still pervasive threats.

Economic crimes fundamentally threaten the basic processes common to all businesses: buying and selling, paying and collecting, importing and exporting, growing and expanding. All organisations, in the course of their daily business, face exposure to various types of economic crime from multiple angles that threaten these activities as they interact with third parties to create or exchange value.

Our hope is that this report will serve all your stakeholders, from the board down, as both a useful reference point in an unending campaign against economic crime and a useful tool in your business arsenal in the months to come.

Trevor White

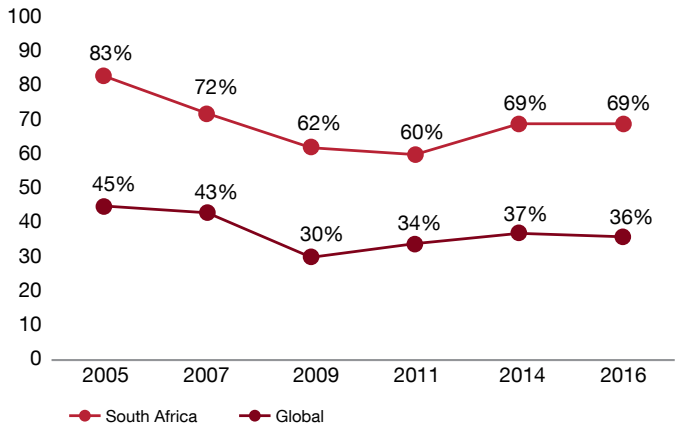
Trevor White
Partner, Forensic Services
PwC South Africa
Global Economic Crime Survey Leader

General economic crime statistics

Economic crime continues to be an obstinate threat in 2016

Economic crime remains a serious challenge to business leaders, government officials and private individuals in South Africa. In this survey we found that the trend has remained unchanged from 2014, with 69% of South African respondents indicating that they had experienced some form of economic crime in the 24 months preceding the survey. When compared to the global statistic of 36%, we are faced with the stark reality that economic crime is at a pandemic level in South Africa.

Figure 1 Reported economic crime rate



Whilst the global trend moved marginally down, South Africa saw the prevalence of economic crime retaining its already high 2014 level of 69%. There is a fear that unless drastic action is taken to curtail the current economic crime trend, we may very well experience an upsurge toward the kind of levels that were experienced when our first Global Economic Crime Survey was carried out in South Africa more than a decade ago. South African respondents reported the highest percentage of economic crime in the world, with France coming in at a close second, followed by Kenya and Zambia. This does not make for good reading from the perspective of the African continent.

Top ten countries reporting most economic crime

1	**South Africa**	**69%**
2	France	68%
3	Kenya	61%
4	Zambia	61%
5	Spain	55%
6	United Kingdom	55%
7	Australia	52%
8	Russian Federation	48%
9	Belgium	45%
10	Netherlands	45%

However, when looking at the list of the other countries reporting the highest rates of economic crime, we also see the likes of Spain, the United Kingdom, Australia and the Netherlands. The fact that included in the top ten reporting countries are what are considered to be developed countries brings home a clear message that economic crime is a global issue and one that affects developed markets as much as it does emerging ones.

Economic crime a global problem, but not the same everywhere

Region	Reported economic crime in 2016	Reported economic crime in 2014
Africa	57%	50%
Western Europe	40%	35%
North America	37%	41%
Eastern Europe	33%	39%
Asia Pacific	30%	32%
Latin America	28%	35%
Middle East	25%	21%
Global	**36%**	**37%**

Breakdown of economic crime types

Signs of evolution as traditional economic crime types give way to high-impact threats

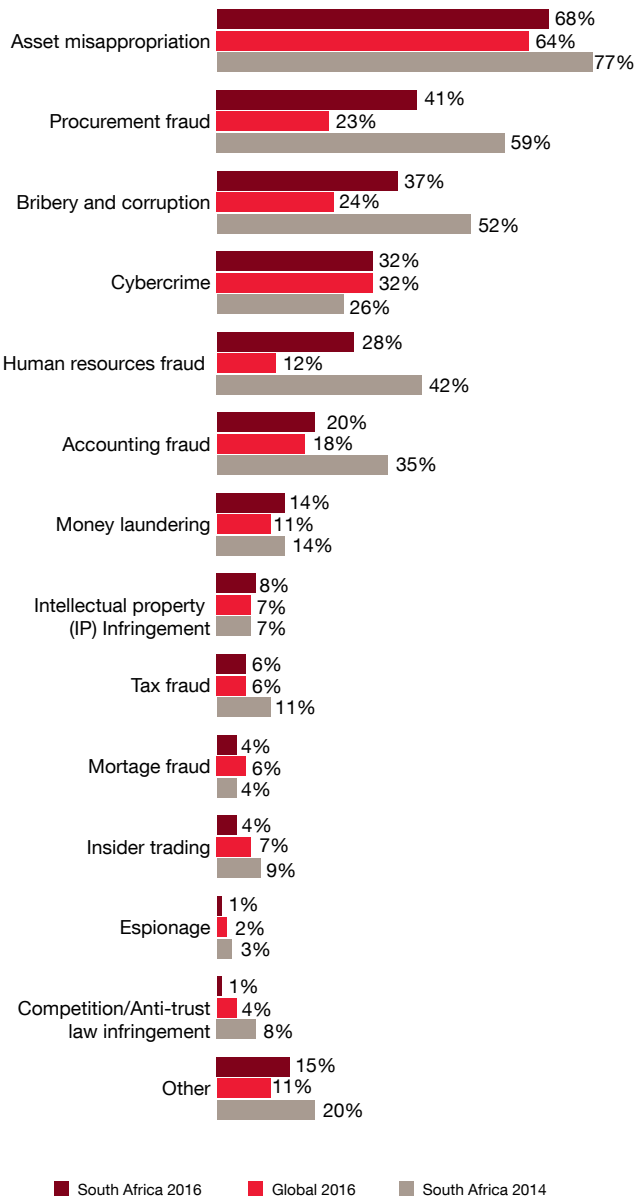
Ever since our first Global Economic Crime Survey in 2003 we have almost been able to guarantee that certain economic crime types will always feature as being the most pervasive. Asset misappropriation, procurement fraud, and bribery and corruption have always been front and centre. Because readers become so accustomed to these 'normalcies', we may sometimes succumb to selective attention, and the stealth with which emerging threats rise could make them too elusive to be noticed. This year's statistics beg a closer look.

Our traditional leaders in the economic crime categories were noted to report lower rates than previously. In fact, the reported rates of economic crime by category this year showed diminished instances for almost every category, even although the average did not decrease. The significant exception is cybercrime, which we explore in greater detail later in this report. This category showed a 23% increase over 2014's rate.

We need to pay closer attention to an evolution of economic crime that may be taking place right in front of us, and try to determine what the underlying reasons are for the changes. Could it be that the reversal of fortune insofar as traditional frauds are concerned is as a result of the tightening of organisational controls whereby organisations are getting better at preventing traditional economic crimes, or are we witnessing an evolution of sorts whereby these crimes are taking on the guise of higher-impact threats such as cybercrime?

From a South African perspective the top seven most reported types of economic crime in South Africa show higher reported levels than the global average, with the exception of cybercrime, which is on par with the global figure.

Figure 2 Types of economic crime experienced over the past 24 months



Detection of economic crime

Detection must be done actively, not passively

The detection of economic crime has presented some interesting anomalies. Despite advancements in technology and an increased dependency on data, detection through data analytics (at 4%) and fraud risk assessments (at 8%) has more than halved in the last 24 months. This comes as no surprise, given that more than one in five organisations (22%) have not carried out a single fraud risk assessment in the same period.

Detection by methods within management control together with those driven by corporate culture both showed declines of 21% when compared to 2014. Our statistics show that over the past two years there appears to have been an increased tendency by both organisations and individuals to be passive in the face of economic crime.

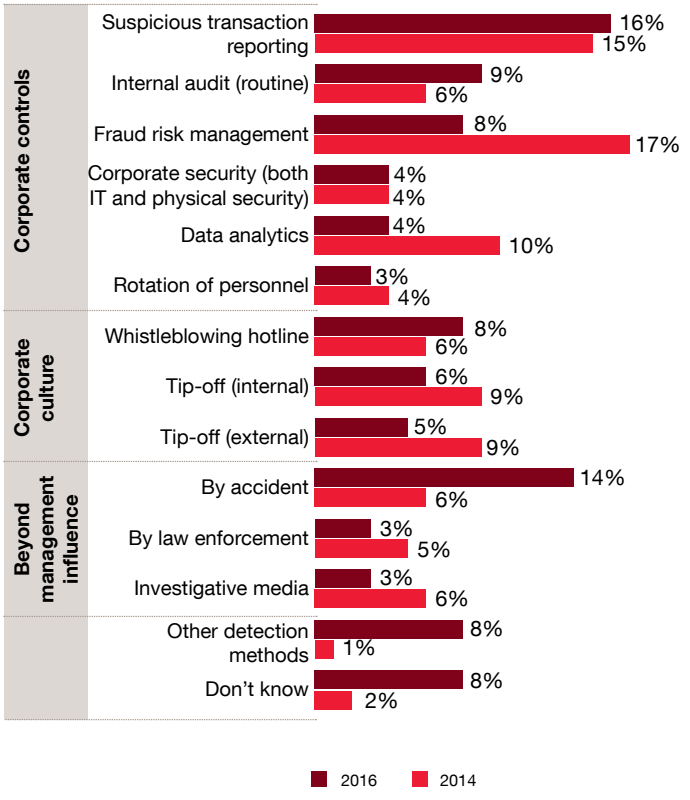
'Today, more than ever before, a passive approach to detecting and preventing economic crime is a recipe for disaster.'

Dion Shango, *PwC CEO for Southern Africa*

Whilst there may be hope in the fact that there has been increased detection by means of whistleblowing hotlines, far too much, it seems, is being left to chance – economic crimes discovered **by accident** more than doubled from 6% in 2014 to 14% in 2016. Another 8% of our respondents could not even tell us how serious economic crimes perpetrated against their organisations were detected.

With the increased levels of focus in recent years on the responsibility (and in many cases personal accountability) of management and boards insofar as good corporate governance practices are concerned, ignorance of matters affecting your company, and specifically a passive approach to detecting and preventing economic crime, is not an option – it is an open invitation for disaster, not only from a corporate perspective but on a personal level as well.

Figure 3 How economic crimes were initially detected in the last 24 months



Blowing the whistle making a comeback?

Much concern has been expressed in recent years about the reduction in instances of economic crimes that are detected by means of whistleblowing. Suggestions have been made that this phenomenon may be the result of widespread distrust of management – and thus resultant distrust of any structures seen to be instituted by management – and fears of the victimisation of would-be whistle blowers. This year's survey results showed a small increase to 8% in the number of economic crimes that were reported by whistle blowers over the last two years, which represents a welcome reversal of the reducing trend witnessed in previous years. Is this a sign of growing confidence within society of being able to do the right thing without fear of reprisal?

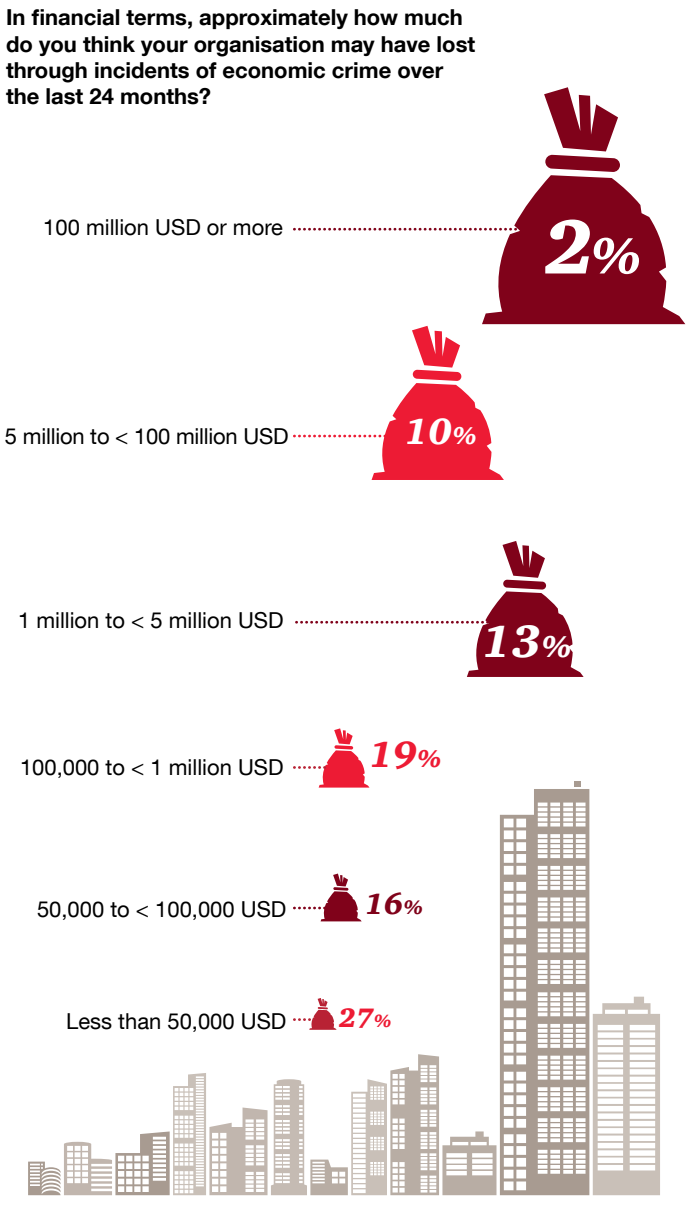
Cost of economic crime

Crime makes you pay, and it costs South Africa billions

While more than half of the global organisations surveyed (53%) reported having lost less than $100 000 to economic crime over the last 24 months, only 43% of South African organisations could make that claim. Almost a fifth (19%) of South African respondents experienced losses of between $100 000 and $1 million, one in four respondents indicated having suffered losses of more than $1 million, and 2% lost in excess of $100 million (double the global average).

It appears that South African organisations are squarely in the cross-hairs of economic predators and are being exposed to greater levels of high-loss incidents than their global and even their African counterparts. And this does not even take into account the true cost of economic crime, which is difficult to estimate since it must consider the collateral damage that ensues from an incident or series of incidents. This includes, but is in no way limited to, business disruptions, consequent interventions required, legal and regulatory costs and the impact on the human and reputational elements comprising a business ecosystem.

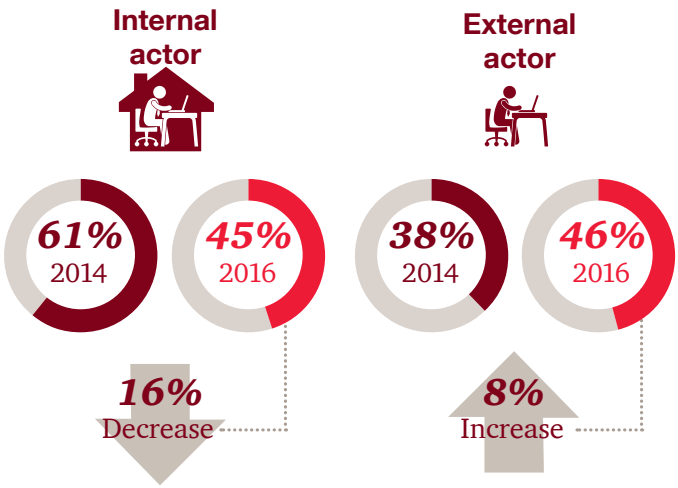
Figure 4 Financial impact of economic crime



Profile of the fraudster (internal and external)

The (not so) usual suspects

This year's survey saw the South African profile of a fraudster taking a quantum leap: for the first time since 2009, external actors exceeded internal actors (albeit marginally so) as the dominant profile of fraudsters acting against an organisation (46% external versus 45% internal). What's more, South African organisations were reported to be more than twice as likely to be defrauded by vendors compared to the rest of the world.

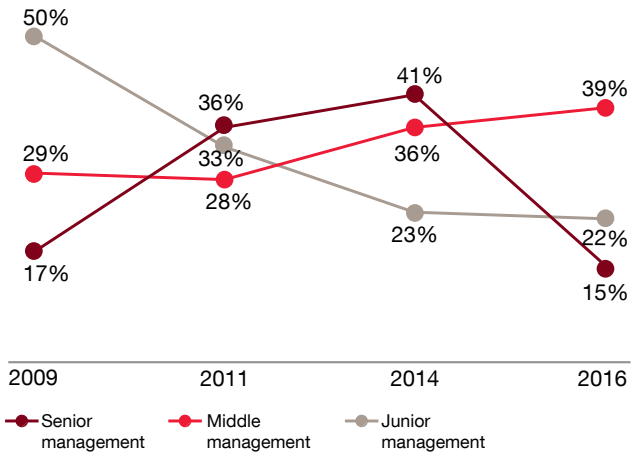


This bears further testimony to the need for ongoing, proactive measures to be in place across the full spectrum of your organisation. Knee-jerk reactions to popular trends at any given time, such as tightening up on managing risks emanating from internal perpetrators, fail to recognise the evolutionary and adaptive nature of economic crimes and the criminals that perpetrate them, whether they are within the confines of your walls or waiting at the gates. Complacency at any level will render your business exposed, because both internal and external perpetrators have a very distinct common trait – they are not part of your organisation, they are against it.

The enemies within

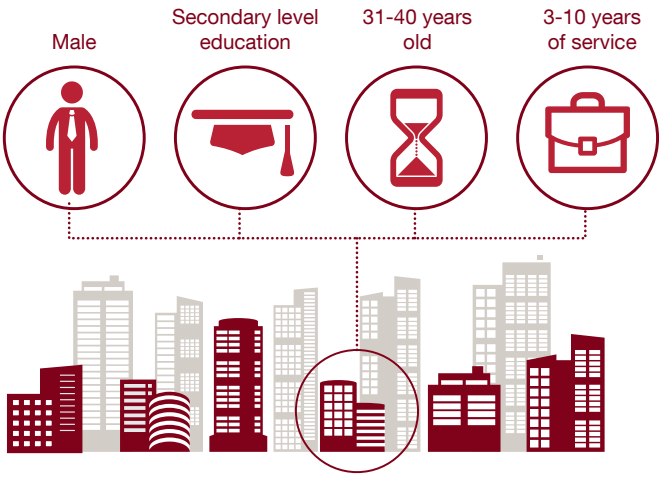
Reports of senior management perpetrating economic crimes against the organisations they work for more than halved from the previous survey (from 41% to 15%), whilst middle management appear to have taken centre stage, with 39% of fraud being perpetrated by internal actors emerging from this band. Whilst on the face of it the dip in the number of senior managers being implicated seems a comforting statistic, the fact that frauds perpetrated by senior management are the hardest to detect raises the question of whether the shift is an actual drop in criminal activity by senior management or points to these occurrences becoming harder to detect because of the control, power and influence that senior management hold. This presents a huge problem for organisations and one which has to be addressed by actively setting up their people and culture as a key proactive first line of defence; making use of alternative detection methods (e.g. data analytics and transaction monitoring tools which are more difficult to circumvent); and dynamically focusing and, as required, refocusing organisational resources and control structures to address their greatest risks, no matter what forms such risks take or where they emanate from.

Figure 5 Historical view of level of internal perpetrator in SA



For control processes to be effective, they must be embedded within an organisation's culture. Every fibre of a business must exemplify its ethos, rather than the business merely paying occasional homage in order to pass a review. Now more than ever, organisations have the opportunity to rethink their control structures and go back to fundamentals.

Mostly likely characteristics of an internal fraudster



The makings of a solution?

Creating a culture of controls and risk awareness rather than ritualised activity, supplemented by zero tolerance for dishonest practices, can help insulate organisations from avoidable losses caused by internal fraud.

The fact that the vast majority of respondents (72%) cited opportunity to commit the crime as the factor that contributed most to the perpetration of economic crime by internal parties points to weaknesses in internal controls and a misguided view of the longevity of established controls.

Given the profile of the typical fraudster, with more than half of them (52%) having reported to have been an employee for between three and ten years, and the stated seniority of these individuals, the controls environment in place may likely not only be familiar to these perpetrators – they may very well have been the architects thereof.

Figure 6 Factors that contributed most to the perpetration of internal fraud

The added dimension that fraud risk assessments are rarely, if ever, undertaken at almost two-thirds (65%) of South African organisations and data analytics has seen a drastic decline in efficacy (detecting only 4% of serious economic crimes in 2016 as opposed to 10% during the previous survey period) points to organisations becoming complacent and dropping the ball when it comes to actively and appropriately managing fraud risks.

This is further demonstrated by the initial response of South African organisations when faced with a potential fraud event. Two-thirds of respondents indicated that they would use internal resources to carry out an investigation (this is a marked improvement from the 75% that took that route in our 2014 survey), but it seems that rather than engaging specialists in the field, South African respondents are starting to lean toward consulting with their auditors and lawyers .

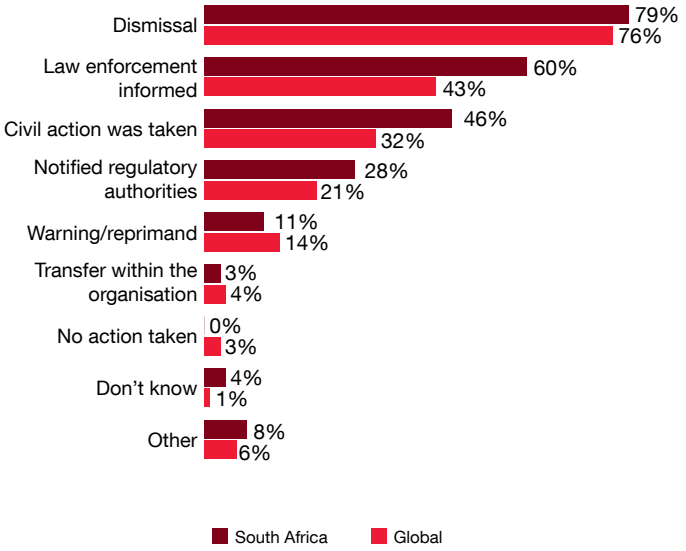
There has been a 1% decrease in respondents engaging a forensic investigator and 2% and 5% increases in respondents consulting with their auditors and legal advisors respectively over the same period.

Given the nature of economic crime and the tendency of mishandled evidence to be regarded as tainted and largely inadmissible, who is approached for assistance or whether the incident is investigated internally is a critical decision that could have a significant impact on the outcome.

A further indicator of the fact that management have had enough is the actions undertaken against perpetrators. In South Africa, as in the rest of the world, dismissal seems to be the most popular approach, but it is very evident that South African organisations are much more likely to also take decisive action.

South African respondents are much more likely to report criminals to law enforcement authorities and regulatory bodies and to take civil action against the perpetrators of internal fraud – this, despite the lack of confidence held in the skills and resources of local law enforcement agencies.

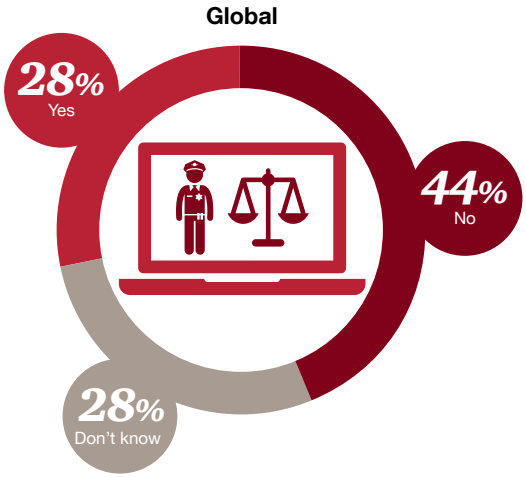
Figure 7 Actions taken against main internal perpetrator

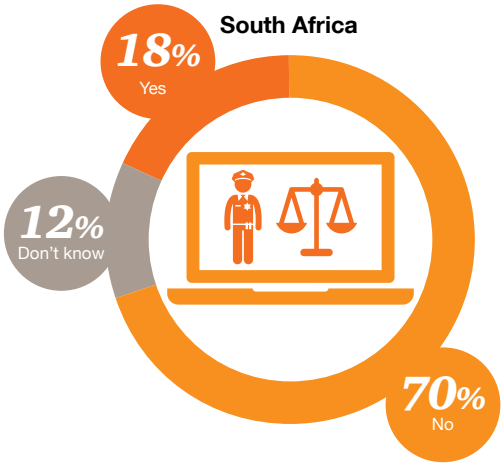


Are we so different after all?

For the first time in our survey, we asked respondents to share their views on whether they believed local law enforcement agencies are adequately resourced and trained to investigate and prosecute economic crime. Whilst it was no surprise that South Africans exhibited a poor perception, the extent thereof was alarming. With 70% of respondents reporting a negative response to the question posed – almost twice the global rate of 44% – South Africa was ranked as the second-highest in the world (second only to Kenya). On closer scrutiny, a few interesting revelations emerge; a myth is dispelled; and several questions are raised.

Figure 8 Do respondents believe local law enforcement agencies are adequately resourced and trained to investigate and prosecute economic crime?





When analysed in comparison with the reported rate of economic crime experienced, we find that a relationship emerges, albeit not a perfectly correlated one, between countries exhibiting low confidence levels in the skills and resources of local law enforcement agencies and those reporting higher rates of economic crime. This may provide interesting insights into, and may also partly explain, the sentiments expressed. Perhaps the negative sentiment is the result of dissatisfaction felt at the outcome of crimes reported, or because of a lack of visibility or understanding of how the judicial systems operate. Or perhaps it is a chicken-and-egg scenario, with high rates of reported economic crime creating negative sentiment while at the same time negative perceptions of law enforcement are creating disillusionment. To add to this toxic potion, victims of economic crime may also inadvertently and unwittingly be contributing to legal actions against perpetrators being rendered unsuccessful (see sidebar, *'So I found fraud…what now?'*).

Top 15 countries reporting economic crime

South Africa	**69%**
France	68%
Kenya	61%
Zambia	61%
Spain	55%
United Kingdom	55%
Australia	52%
Russian Federation	48%
Belgium	45%
Netherlands	45%
Ukraine	43%
Luxembourg	42%
Switzerland	41%
New Zealand	40%
Chile	39%

Top 15 countries that believe that their local law enforcement agencies are not adequately resourced and trained to combat economic crime

Kenya	79%
South Africa	**70%**
Turkey	60%
Philippines	58%
Bulgaria	58%
Poland	58%
Ukraine	57%
Mexico	56%
Zambia	55%
Nigeria	54%
Australia	52%
United States	52%
France	51%
Venezuela	50%
India	49%

A commonly held and oft-repeated opinion that has reached myth status is that these negative sentiments only occur in emerging markets or developing countries. It is assumed (perhaps because of perceptions created through the media and no doubt bolstered through cinema) that developed countries have law enforcement agencies that are flawless and have access to unlimited resources. It is further presumed that every citizen shares this view. On the contrary, though, our global survey uncovered a widespread lack of confidence in local law enforcement agencies — a phenomenon that is not limited to regions or level of economic development. It is, of course, conceivable that this metric could have resulted from several divergent factors, including countrywide rates of economic crime, the extent to which law enforcement agencies in the respective countries publicise or (even) downplay their expertise in certain areas like cybercrime, and the extent to which law enforcement agencies are perceived to be above political interference.

'With local law enforcement agencies being perceived to be under-resourced and under-trained to tackle economic crime and make a material difference, the onus is squarely on the shoulders of the business community to protect itself and its stakeholders.'

Louis Strydom, *PwC's Africa Forensic Services Leader*

So I found fraud...What now?

Your initial response to a fraud event may very well determine the final outcome and the fate of the perpetrator/s. Incorrect procedure, lack of objectivity and poor handling of evidence may lead to court actions being bungled and failing on technical grounds. With **less than half** of South African respondents indicating that they engage appropriately skilled specialists and **two-thirds** attempting to do it in-house, are the odds for successful prosecutions stacked in your favour or are they against you?

Combination of actions taken by respondents once a potential fraud is detected:

HR fraud

Clampdown on bogus qualifications overdue

Of the respondents that experienced human resources fraud, an overwhelming 68% reported being victimised through the submission of false qualifications. This is significantly higher than the global average of 44% and almost double the next-highest type of human resources fraud suffered by South African respondents, namely false wage claims (39%).

Figure 9 Types of human resources fraud

Government and state-owned entities have been plagued by numerous high-profile scandals involving falsified qualifications in the past couple of years, and there seems to be no end to the number of people who are prepared to take a chance and lie about their qualifications to get a job or a promotion. Senior officials in crucial positions have lied about their qualifications and then scrambled to find non-existent certificates when this was exposed in the media. While this scourge is often referred to as 'educational misrepresentation', it is nothing less than fraud and needs to be dealt with as such if it is to be stopped and those who have studied diligently and obtained university degrees are to be justifiably rewarded.

As can be seen from our survey results, with respondents hailing predominately from the private sector (83%), the crime of misrepresenting qualifications is not limited to the public sector. Companies are, however, very wary of the reputational damage that negative publicity of this nature could have on their image and brand and therefore try and ensure that this is not disclosed to the media and public.

Employers in both the public and private sectors, institutions and citizens need to jointly take a tough stance that this type of fraud will be dealt with to the fullest extent of the law, with the perpetrators being charged, prosecuted and, if appropriate, even imprisoned.

How to limit qualification fraud

When your business is recruiting for a position that requires an academic qualification, it is not enough to simply trust that a candidate has the qualification they claim to have. A business has to have a clear policy regarding pre-employment screening that covers at least the following to ensure they do not end up with the embarrassment of employing unqualified applicants:

- Screen **all** potential employees, whether permanent staff, contract or temporary workers.
- Perform screening of tertiary qualification/s, membership of professional association/s and employment history; and carry out credit and criminal background checks.
- Ensure the application form requests all relevant information, including consent for checks.
- Be clear about how you will deal with false or forged documents.

Procurement fraud

Maintaining focus on procurement fraud

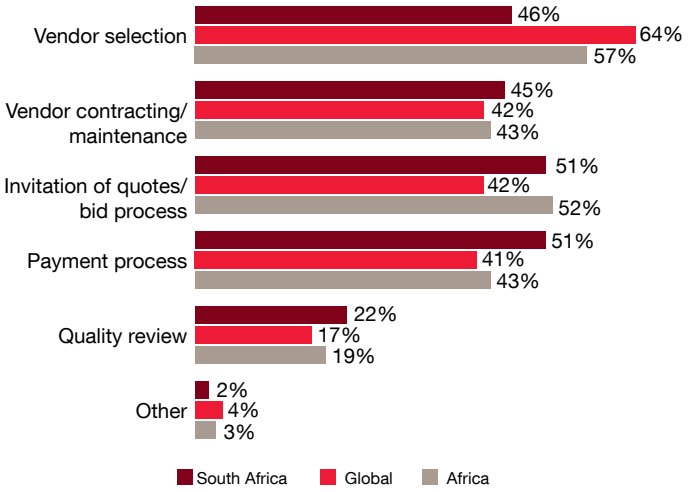
Procurement fraud is still the second most reported type of economic crime in South Africa, with 41% of respondents having been victims of this type of crime in the past 24 months. While this is down from prior years, it is still almost double the global average of 23%.

Procurement fraud can be defined as the unlawful manipulation of the procurement cycle by service providers and in-house personnel to procure goods and/or services, obtain an unfair advantage, circumvent an obligation or cause a loss to an organisation.

There are various statutes in South Africa that affect how procurement is undertaken in particularly the public sector, but also the private sector. These include the Prevention and Combating of Corrupt Activities Act 12 of 2004 (as amended), the Public Finance Management Act 1 of 2009 (as amended) and the Municipal Finance Management Act 56 of 2003, which criminalise corruption and are aimed at eliminating waste and corruption in the use of public assets, ensuring government transparency and enabling public sector managers to manage, but simultaneously be held more accountable.

Whilst our results show an 18% decline in the reported occurrences of procurement fraud, when overlaid with the number of internal perpetrators emanating from senior and middle management – the very same group charged with managing the procurement cycle – the stark reality emerges that the very people who are tasked with overseeing the procurement process may very well be perpetrating the economic crimes themselves. Senior and middle management fraud is by its very nature harder to detect, and even when it is detected it is harder to take action against the perpetrators.

Figure 10 Areas where procurement fraud occurred



Where does Procurement Fraud occur?

A closer look at the areas where procurement fraud was noted to have been carried out confirms the age-old suspicion that there is collusion between procurement officials and suppliers most of the time:

- Bid rigging/Bid splitting
- Creating 'shelf companies' to facilitate fraudulent payments
- Collusion between service providers or between service providers and employees
- Purchase orders and/or contract variation orders which have not been approved and/or authorised by the designated official
- Unjustified single-source awards
- False invoices for products and/or services for non-existent vendors
- Bribery during the awarding of contracts.

Cybercrime

Although military assets are assumed to be highly secure, hackers have found that low risk suppliers have gaps in their security, which can be easily exploited and used to track the destination of these supplies.

A threat that knows no boundaries

Digital technology continues to transform and disrupt the world of business, exposing organisations to both opportunities and threats. So it's hardly surprising that cybercrime continues to escalate — ranking as the second-most reported crime in this year's Global Economic Crime Survey and taking fourth place from a South African perspective. At 32%, it was the same as the global average.

The reality in 2016 is that, like every other aspect of commerce, economic crime has to some extent gone digital. In a hyper-connected business ecosystem that frequently straddles jurisdictions, a breach in any node of that system — including third parties such as service providers, business partners or government authorities — can compromise the organisation's digital landscape in a variety of ways. What's more, cyber risk now encompasses more than our traditional view of computers: we've observed a sharp increase in attack activity involving the Internet of Things, including cars and household devices.

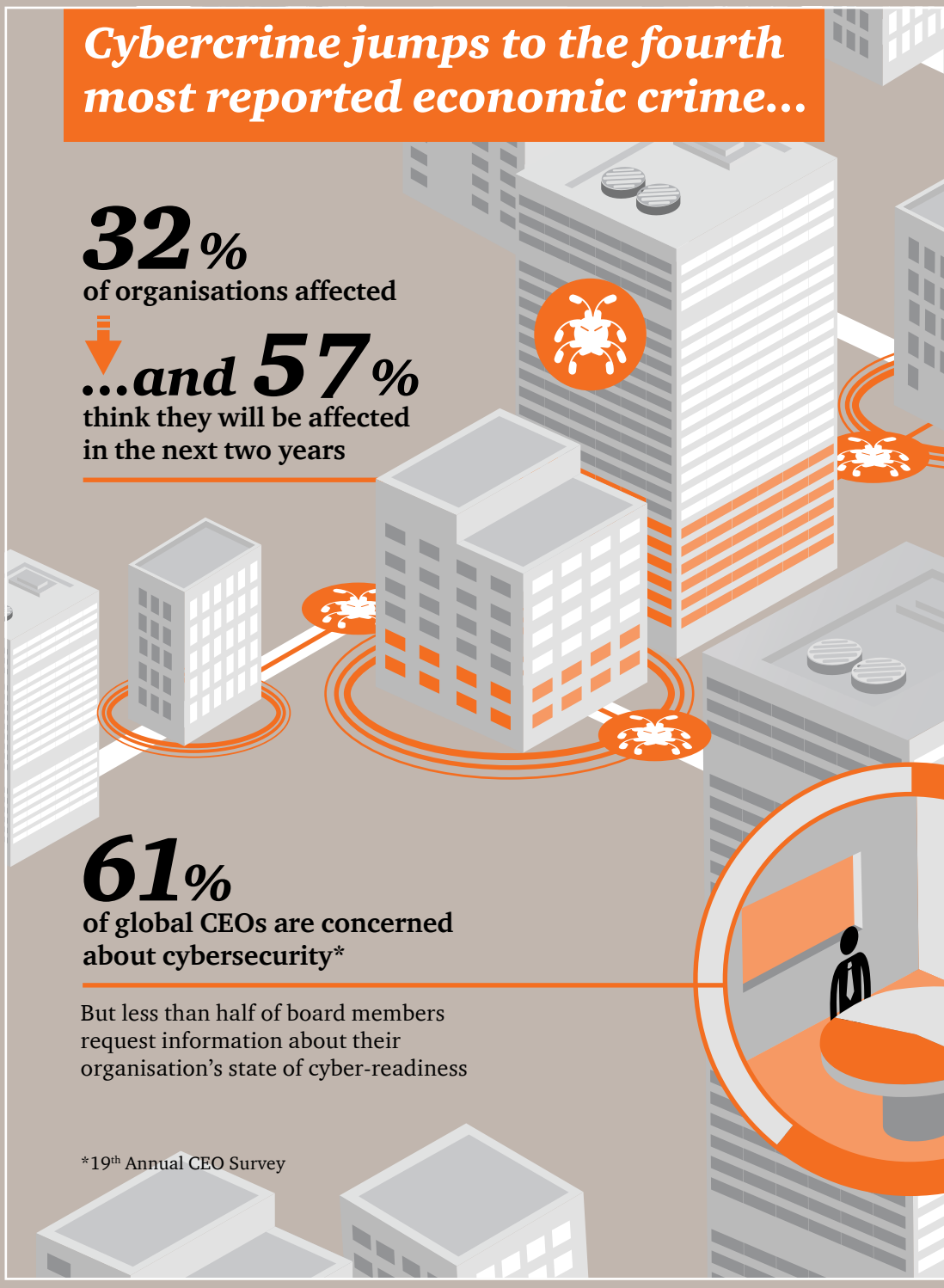
Here's the digital paradox: Companies today are able to cover more ground, more quickly, than ever before thanks to new digital connections, tools and platforms which can connect them in real time with customers, suppliers and partners. Yet at the same time cybercrime has become a powerful countervailing force that's limiting that potential.

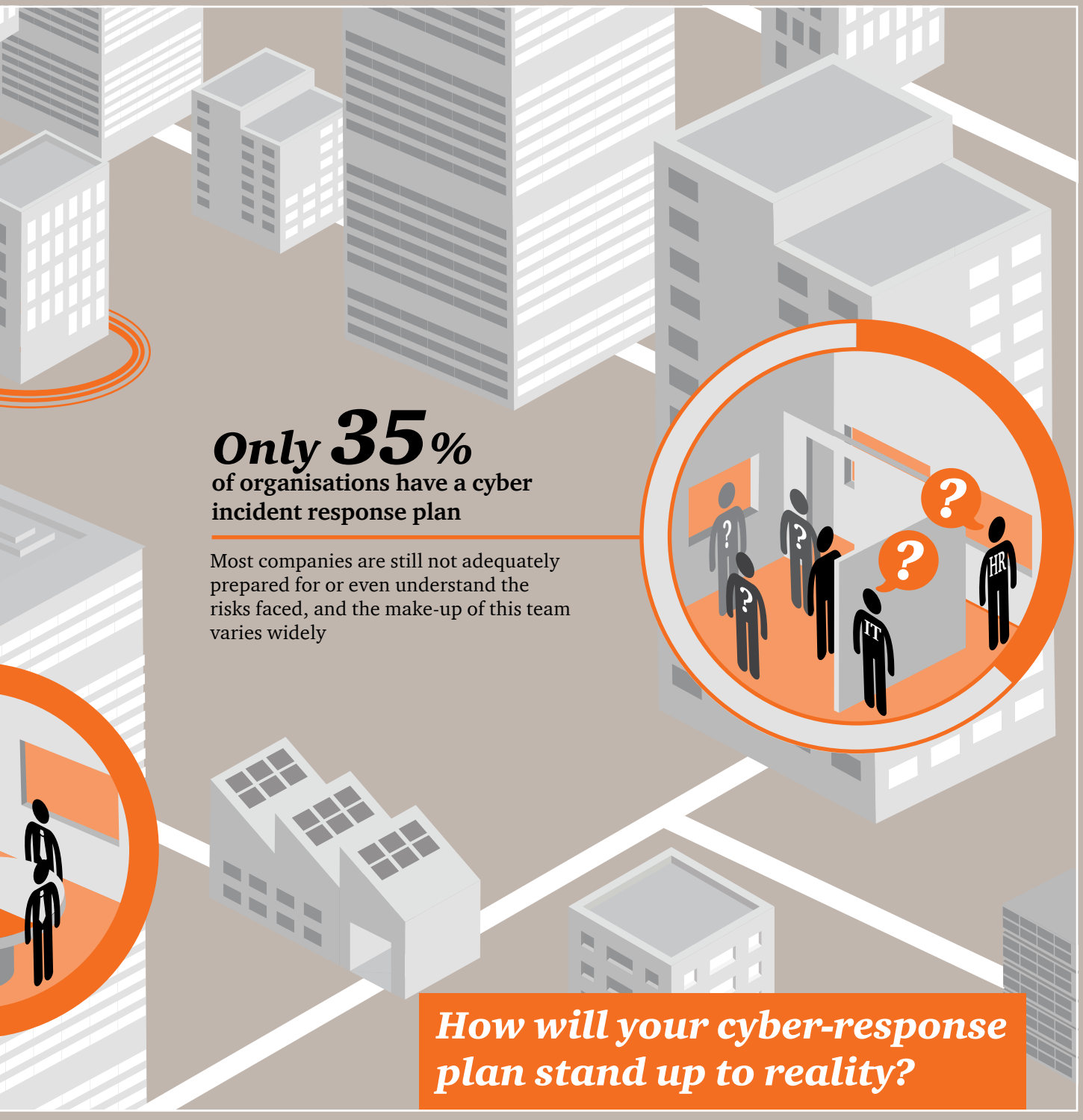
And business leaders worry it's holding them back. In PwC's 19th Annual Global CEO Survey, six in ten chief executives ranked cyber threats and the speed of technological change as top threats to growth.

This year's survey points to the disquieting fact that too many organisations are leaving first response to their IT security teams without adequate intervention or support from senior management and other key players. What's more, the composition of these response teams is often fundamentally flawed, which ultimately affects the handling of breaches.

From our firm-wide work on digital strategy and execution with thousands of companies globally, we've identified practices that distinguish leaders in the digital age. Chief among these is *a proactive stance when it comes to cybersecurity and privacy*. This necessitates that everyone in the organisation — from the board and C-suite to middle management and hourly workers — see it as their responsibility.

Cybercrime continues to escalate in a hyperconnected business ecosystem – jumping to 4th most reported economic crime





Only 35%

of organisations have a cyber incident response plan

Most companies are still not adequately prepared for or even understand the risks faced, and the make-up of this team varies widely

How will your cyber-response plan stand up to reality?

Cybercrime keeps climbing

The incidence of reported cybercrime among our respondents is sharply higher this year, with a 23% increase from the previous survey conducted in 2014. So although cybercrime in the South African context has shifted two places from sixth to fourth position, it is the percentage increase that is more concerning. A third of respondents told us they'd been affected by cybercrime. Ominously, another 16% said they didn't know whether they had or had not been victims of cybercrime.

In terms of losses, at least 3% of respondents that were victims of cybercrime had experienced financial losses greater than $100 million, whilst 27% experienced losses between $1 and $50,000. Again, a sobering statistic is that 14% of respondents don't know or were unable to quantify their financial losses even though they had been victims of cybercrime.

Case study: Leaving the front door unlocked?

The incident below is loosely based on an actual investigation conducted. Some details have been changed in order not to divulge the identity of the organisation.

We received a panicked call from an organisation requesting first-responder capabilities to assist with an incident that was 'detected'. An anonymous tip-off had been sent to our client informing them that they were being hacked on a regular basis by a competing organisation.

Over the next few days evidence from our client's systems was obtained confirming that the anonymous tip-off was actually correct. Based on the evidence obtained we were able to assist our client's legal advisors in launching a civil application to conduct a search of the competitor's business premises, one of the competitor's branches and the holiday home of one of the competitor's directors.

Evidence obtained during the search showed that ten computers had been used to access our client's systems over 3 000 times over a six-month period, exfiltrating critical customer and other high-value data assets.

A financial settlement in favour of our client was eventually reached by the parties.

So what about the front door? – From a digital forensics perspective this matter would not technically be classified as a hacking incident. Staff members had merely left the employment of our client, moved to the competitor and continued to have access to our client's systems. It was a simple control failure where IT failed to de-activate the accounts of ex-employees.

The alarming thing about this is that we see a number of breaches of this nature annually where the very basics of security have been ignored. As in the above incident, almost all organisations we've seen were alerted by external factors and not their internal monitoring processes.

Among survey respondents in South Africa, financial losses were considered to be the most damaging impact of a cyber breach, followed closely by legal implications and reputational damage. This differed from the global perspective, where reputational, legal and regulatory impacts were considered to be the most significant.

The insidious nature of this threat is such that of the 46% who say they are not victims, many have likely been compromised without knowing it. A concerning trend we have observed is that of hackers managing to remain on organisations' networks for extended periods of time without being detected.

'Today's adversaries are so skilled at exploiting code and obfuscating their actions that many companies cannot discover a breach until months or even years after the initial attack.'

David Burg, *PwC's Global and Co-US Cybersecurity Leader*

Attackers are also known to stage diversionary attacks to conceal more damaging activity. Diversionary techniques include use of distributed denial of service attacks as a means of distraction and creating a lot of noise while the real focus of the attack unfolds in a slow and undetected manner. Typically, in such a scenario attackers would launch attacks against systems which provide no value to them. This is done simply to misdirect incident response teams, though, whilst in the background attackers are attacking and exfiltrating the actual information they are seeking. Such techniques would typically be used against organisations that have strong security and incident response teams. Organisations who leave the proverbial 'front door' open are subject to less sophisticated attacks which are equally damaging, and unfortunately in the South African context when conducting investigations, we find a number of organisations falling into this category. After all, why would an attacker expend energy and time to tackle sophisticated defences when basic security practices have been ignored?

The two kinds of cybercrime and what they mean for you

We've come a long way from the days of juvenile hackers simply crashing systems or changing displays just for a good laugh.

Over the last few years, economic cybercrime has evolved to a point where one could segment it into two distinct categories — the kind that steal money or data that is monetisable and bruise reputations; and the kind that steal IP and lay waste to an entire business. The latter are often classified as transfer-of-wealth attacks.

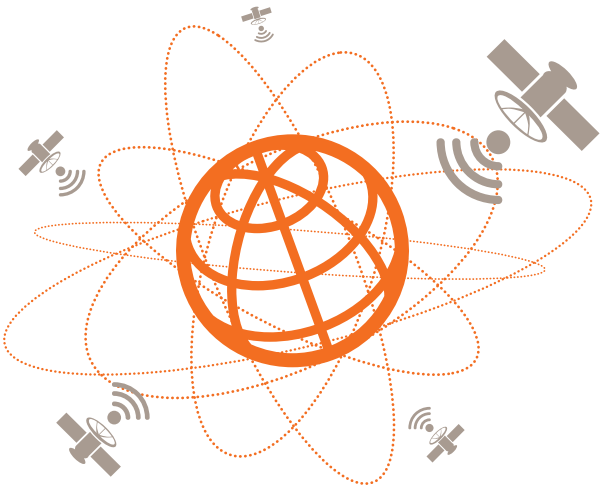
While the long-term damage, both to organisations and the economy, is potentially far higher for transfer-of-wealth attacks, the regulatory pain and media scrutiny arising from the theft of credit cards or personally identifiable information can be damaging too, especially with the promulgation of privacy legislation like the Protection of Personal Information (PoPI) Act and the impending Cybercrimes and Cybersecurity Bill. South African organisations will increasingly find themselves having to deal with regulators in the event of an incident occurring.

Threat vectors: the five categories

Nation-states
threats include espionage and cyber warfare; victims include government agencies, infrastructure, energy and IP-rich organisations

Insiders
not only your employees but also trusted third parties with access to sensitive data who are not directly under your control

Terrorists
still a relatively nascent threat, threats include disruption and cyber warfare; victims include government agencies, infrastructure and energy



Organised crime syndicates
threats include theft of financial or personally identifiable information (sometimes with the collusion of insiders); victims include financial institutions, retailers, medical and hospitality companies

Hacktivists
threats include service disruptions or reputational damage; victims include high-profile organisations and governments; victims can include any kind of organisation

Why do companies (and nation-states) steal intellectual property?

- Many developed nations are seeing a pattern in large-scale IP-focused breaches. They are not random individual company attacks, but rather parts of a larger-scale, strategically organised campaign.
- While nation-states may be behind some of these large-scale attacks, this is not a terrorism issue (attempting to cripple vital infrastructure), it is an economic crime issue.
- There is an economic rationale in stealing another company's IP. It is less expensive in time and resources than conducting one's own R&D.
- The advice is: If you see someone else in your sector getting attacked, it is wise to assume you may be next.

Ready? Or not?

Almost three quarters of our respondents (69%, a 15% increase on 2014) see an increased risk of cyber threats, perhaps due to intensifying media coverage. A disparity between chief executive officers and chief financial officers was noted in response to this question, with 83% of chief executive officers and only 57% of chief financial officers seeing an increased risk in cyber threats. We see this playing out in terms of boards and CEOs engaging on the subject, but follow-up spending is not always on par with this level of engagement.

Responsibility for redressing cyber vulnerabilities starts at the top. Yet our survey suggests that many boards are not sufficiently proactive regarding cyber threats and generally do not understand their organisation's digital footprint well enough to properly assess the risks, despite the fact that boards have a fiduciary responsibility to shareholders when it comes to cyber risk. As mentioned previously, we are currently seeing related legislation being implemented in South Africa. Only 48% of boards are requesting information around cyber-readiness locally; this is slightly higher than the global average of 43%. In practice, we are also finding that not all boards are requesting the right type of cyber readiness information. More often than not, information presented to boards is linked to compliance and external audit requirements. Internal audit and internal risk functions need to further develop their capabilities in identifying and dealing with cyber threats, which will in turn impact cyber readiness programmes.

Figure 11 Frequency of requests for information by boards regarding organisations' ability to deal with cyber incidents

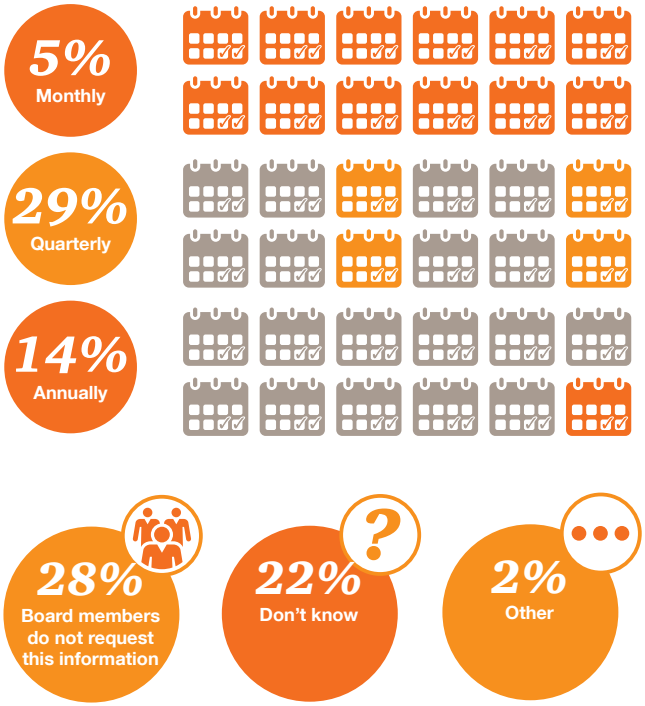


Figure 12 Do organisations have Incident Response Plans to deal with cyber-attacks?

Only 35% of respondents have a fully operational incident response plan; 13% don't know if they have one; and, more astonishingly, 12% do not have one nor do they intend implementing one!

Should a cyber crisis arrive, only 34% of organisations have personnel that are 'fully trained' to act as first responders, and 20% of organisations indicate that they will make use of outsourced personnel. Through the investigations we've conducted we often find that organisations who make use of outsourced digital forensics providers only start procuring services when an incident occurs – and delays in the procurement process often result in a time lag during which critical evidence is lost or damaged. Organisations should ideally be appointing incident response teams on retainer to ensure rapid response times.

Further to this, on examining the composition of incident response teams, we noted that teams are still weighted towards having more IT security personnel (73%) and IT staff (62%), while only 28% of organisations include digital forensic specialists. South African incident response teams still fare better than their global counterparts, however, as only 11% of organisations globally have digital forensics specialists on the team.

These results suggest that many organisations, in their understandable haste to contain the breach and get their systems up and working again, are at risk of overlooking potentially crucial evidence — which could later hamper their ability to prosecute and, more importantly, to understand how the breach occurred.

In the immediate term, an insufficiently coordinated response might also limit the organisation's ability to investigate all the areas that have actually been breached, especially critical considering hackers' frequent use of diversion techniques.

Finally, excessive haste in responding to an attack can hamper the company's ability to fully understand the *holistic impact* of the breach and communicate appropriately with both internal and external stakeholders, including the media. This could lead to reputational harm (ranked in this year's survey as the most damaging impact of a cyber breach).

"We have seen many organisations suffer damaging losses because they simply don't get the cybersecurity fundamentals right.

This basic preparedness includes factors like sufficient board involvement, correct system configurations and adequate controls over third-party business partners that have access to the corporate network.

A lack of these cyber-readiness basics can leave the cybersecurity door ajar for intruders."

Junaid Amra, *PwC Forensic Technology Services*

Figure 12 Cybercrime First Responder Teams

Detecting a breach: Crisis management

What happens when you learn of a breach? It's critical to shrink the interval between effective detection and response – and interrupt damaging business impacts as quickly as possible. After calling up your crisis and cyber first-responders, here are some steps you can take:

- Get the essential facts about the breach, and find out if it is still ongoing. With the increasing complexity of networks, it can be difficult to identify how a hostile actor might have entered the network. In this phase it is also important to understand if the incident response team assembled has the capabilities to deal with the breach on hand.
- Consider that a detected attack can sometimes mask deeper incursions into your organisation, and that in some situations it may take weeks, not hours, to detect a breach and begin to stem the damage.
- Decide whether and to what extent to seek the involvement of law enforcement. There are many factors to consider, and these will vary according to the type and scale of the attack. (This is a significant issue, considering that 70% of responders doubt local law enforcement agencies' capability to investigate cybercrime.)
- Consider secondary risks. For example, a simple email breach can reveal secrets to adversaries. If networks are breached and the company uses a VOIP/networked phone service, the telephones are also likely to be compromised.
- Finally, when a breach occurs, remember: *a cyber investigation is still fundamentally an investigation*, and the principles of a criminal investigation still apply. In focusing on stopping an ongoing attack and getting back on line, it's crucial not to inadvertently destroy evidence that could help with that investigation — and with preventing the next attack.

The importance of a multi-layered defence

Cyber threats and mitigations are the responsibility of the entire enterprise; all have a crucial part to play. Yet while we have seen major strides being made in sophistication and cyber-preparedness since our last survey, most companies are still not adequately prepared for them to either understand the risks they face or anticipate and manage incidents effectively.

Too many organisations are suffering cyber losses because they didn't get the basics right. From insufficient board involvement (or readiness-awareness) to poor system configurations and inadequate controls over third parties with access to the network, companies are suffering from unforced errors, often leaving the cyber door ajar for intruders.

It is vital that boards incorporate cybercrime into their routine risk assessments; communicate the plan up, down and across organisational lines; and discuss specifically with the IT department at what point they want to be alerted of a breach.

Cyber threats must be understood and planned for in the same way as any other potential business threat or disruption (such as acts of terrorism or a natural disaster), involving a response plan, roles and responsibilities, monitoring and scenario planning. That's why leading companies are integrating crisis management exercises as a central element of their cybersecurity and incident response strategy. They convene regular table-top exercises that examine specific scenarios, and pressure-test their response plans to identify any gaps or shortfalls.

Game of Threats ™

In response to this need, PwC has developed a cyberattack simulation tool called The Game of Threats ™ that allows executives to simulate attacks from various threat agents whilst mimicking a real-world scenario. This includes media reports, social media discussions and the financial constraints of specific options during a crisis. The real-world crisis simulation has in our experience changed the perceptions of executives in terms of their readiness to deal with such events.

A cyber corporate crisis is one of the most complex and challenging issues an organisation can face. Cyber breaches require sophisticated communications and investigative strategies — including significant forensic and analytical capabilities — executed with precision, agility and a cool head.

Although potentially daunting, ramping up preparedness has its silver lining: you can view it as an organisational stress test — one that can and should lead to improvements in your processes. In today's risk landscape, a company's degree of readiness to handle a cyber crisis can also be a marker of competitive advantage and, ultimately, its survival.

Plans are good, but practice is everything

Many companies are integrating regular crisis management exercises as a central element of their cybersecurity and incident response strategy. They will convene regular table-top exercises examining specific scenarios, and then pressure-test their incident response plans, identifying any gaps or shortfalls.

Unfortunately, plans rarely survive first contact with reality. Reality tends to present incident responders and crisis managers with unforeseen circumstances.

An effective crisis response requires the skills, knowledge and experience of a range of corporate functions working in concert: legal, human resources, media and public relations, communications, privacy counsel, audit and risk, finance, corporate security, regulatory and law enforcement relations, shareholder relations, as well as the front-line business units and regional management.

The process — the 'plan for a plan' — that comes from a regular exercise programme is far more valuable than the plans it produces. It generates 'muscle memory' for incident response, making the process, the environment and the decision-making construct second nature to the stakeholders, who will be under pressure in a crisis, so they can focus on solving the issue at hand.


THE WALL STREET JOURNAL.

Risk & Compliance Journal.

The Morning Risk Report: Game Helps Companies Confront Cyberattack Realities

BEN DIPIETRO

Wall Street Journal


CORPORATE COUNSEL

Top News

Target Sued Over 'Walk of Shame' Suicide

LSU Brings in Jones Day Partner as GC

Battling Bribery: A Private-Sector Call to Arms

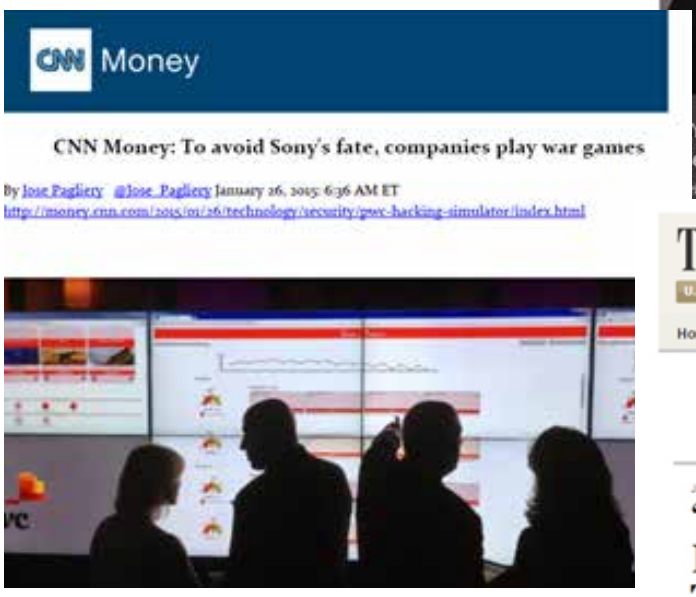
E-signatures: Enhancing the Value of Contract Automation

Banks Want Merchants to Chip In After a Data Breach

Pharma and Biotech Getting in the Postgrant IP Game

urning Cybersecurity Into a erious 'Game of Threats'

icewaterhouseCoopers has created a computer game


CNN Money

CNN Money: To avoid Sony's fate, companies play war games

By Jose Pagliery @Jose_Pagliery January 26, 2015: 6:36 AM ET

http://money.cnn.com/2015/01/26/technology/security/pwc-hacking-simulator/index.html


THE WALL STREET JOURNAL.

U.S. EDITION Friday, January 23, 2015 As of 12:03 PM EST

Home World U.S. Business Tech Markets Market Data Your Money

CIO Journal.

CIO Report Consumerization Big Data Cloud Talent & Management Security

January 21, 2015, 8:07 PM ET

'Game of Threats' Teaches Executives Cyber Readiness Through Game Play

IT threats and mitigations are the responsibility of the entire organisation

Executive level:

- Institute sound cybersecurity strategy
- Ensure quality information is received and assimilated
- Implement user security awareness programmes
- Enable strategy-based spending on security

Legal:

- Track the evolving cyber-regulatory environment
- Monitor decisions made by regulators in response to cyber incidents
- Be aware of factors that can void cyber insurance

Audit & Risk:

- Ensure a thorough understanding and coverage of technology risks
- Conduct up-front due diligence to mitigate risks associated with third parties
- Address risks associated with operational (non-financial) systems
- Address basic IT audit issues

IT:

- Conduct forensic readiness assessments
- Be aware of the changing threat landscape and attack vectors
- Test incident response plans
- Implement effective monitoring processes
- Employ new strategies: cyberattack simulations, gamification of security training and awareness sessions, and security data analytics

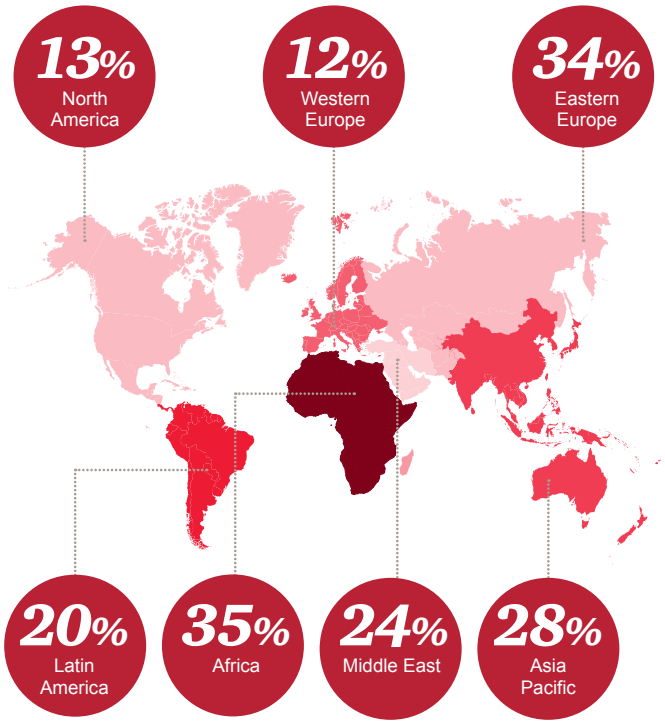
Ethics and compliance

Managing the balance between trust and compliance can be the difference in retaining or losing top talent. In today's continuously evolving marketplace, having a strategy for aligning ethics and compliance with business risks will keep you on the path towards realizing your opportunity

Rooting out corruption is everyone's responsibility

Bribery and corruption are still reported as a major problem by more than a third (37%) of our South African respondents – this, despite heightened publicity and exposure of a number of cases in recent years. When compared to the global average of 24%, the significance of the issue faced by the South African economy is clear and an area for grave concern. But the problem is not only domestic; a review of our global statistics makes it evident that bribery and corruption are still very prevalent in what are considered to be developing markets.

Bribery and corruption by region



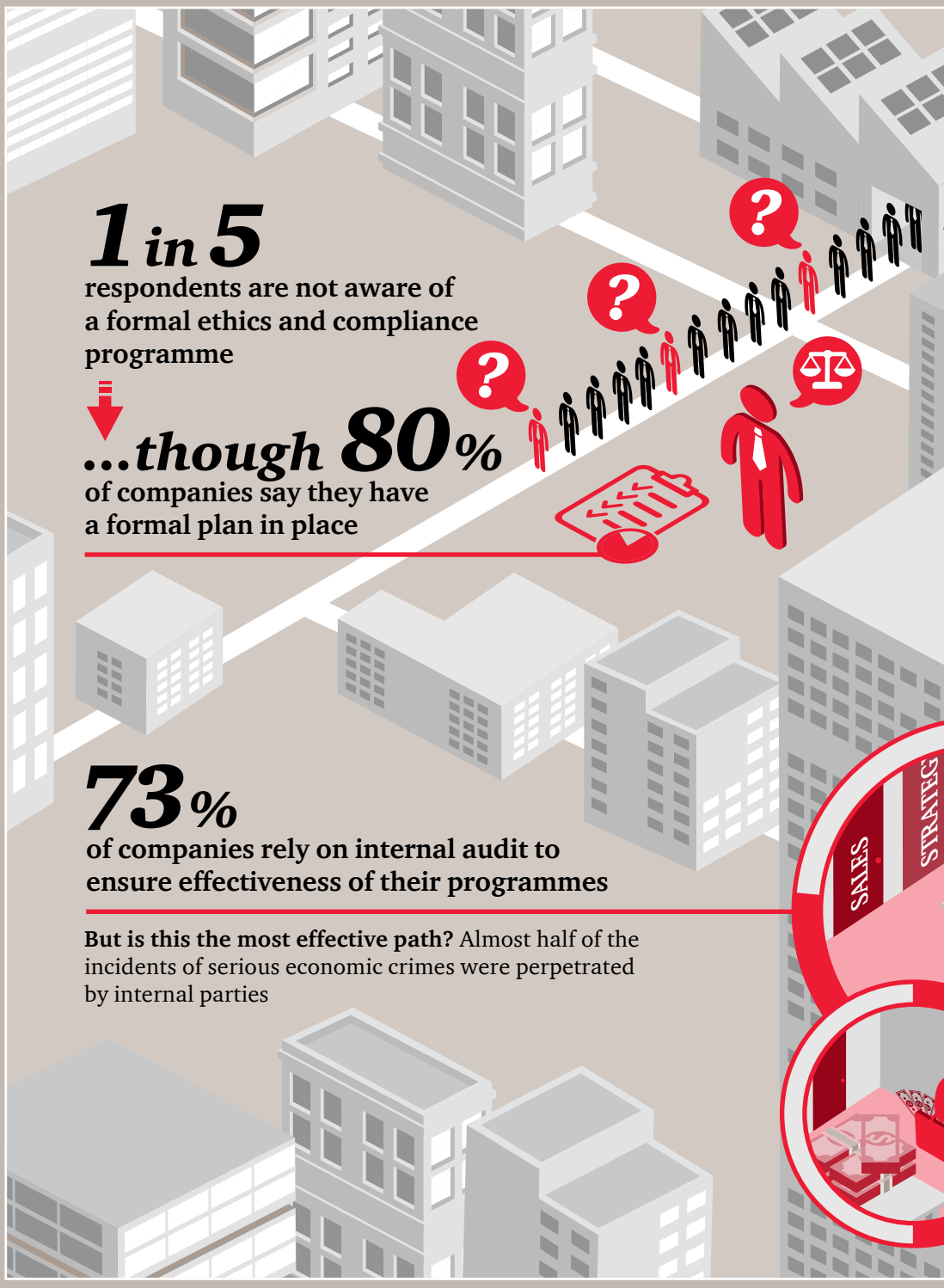
Corruption is defined as a form of dishonest or unethical conduct by a person entrusted with a position of authority, often to acquire a personal benefit. There are many articles and papers that have been written on how to prevent and eradicate corruption. The general consensus among authors on the subject is, however, that corruption amounts to nothing more than greed. The end result is often that the poor are in many cases deprived of basic services such as health care, education and housing. Simply put, corruption is a cancer that is eating at the very fabric of our society.

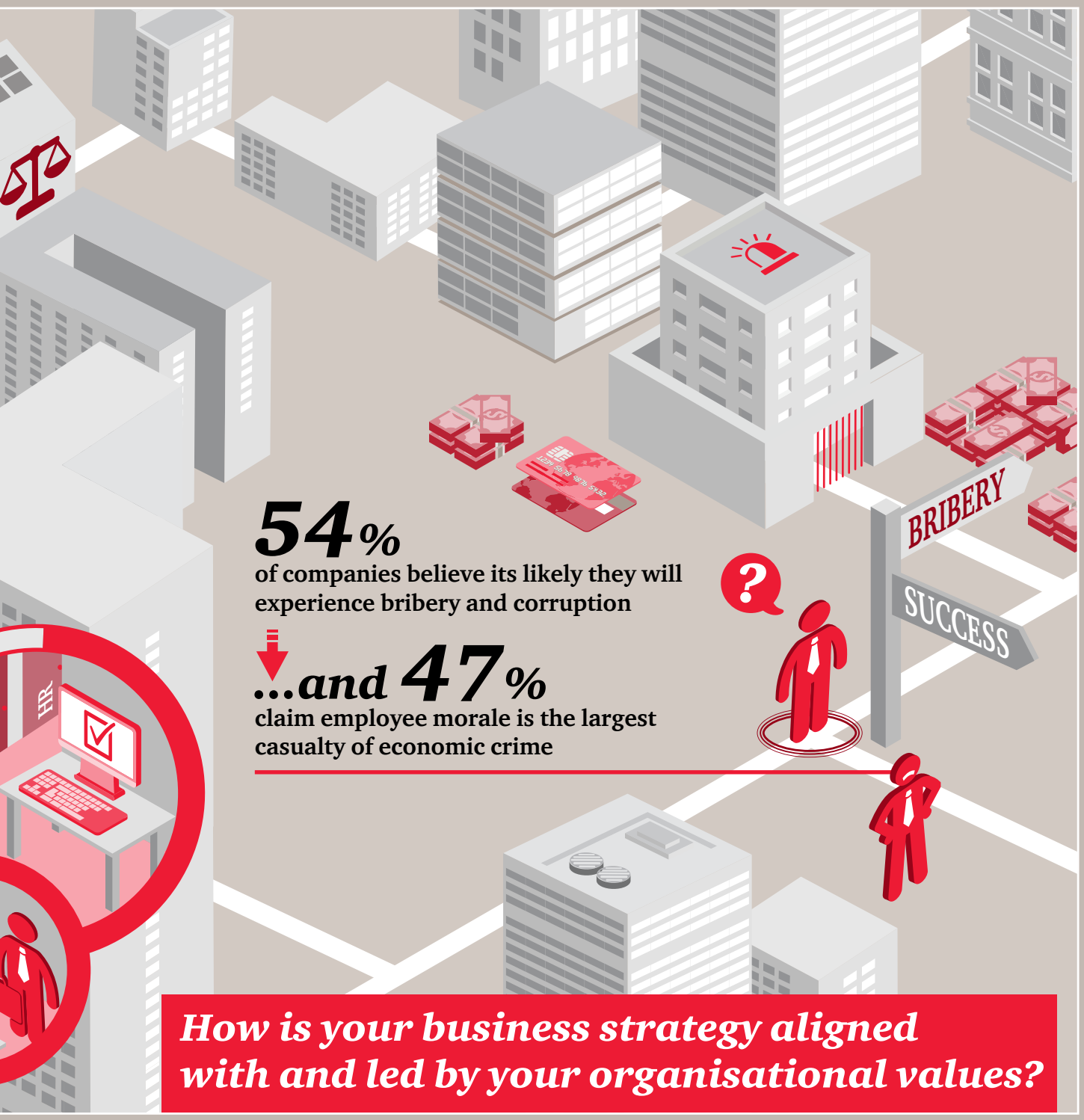
The reality is that for every corruptee that receives a bribe there is a corruptor that is prepared to pay it – both are equally guilty in terms of the law. Instances of bribery and corruption are rife at not only public entities but within the private sector as well. Our findings indicate that one out of every seven (15%) of our respondents, who hail from both public and private organisations, had been asked to pay a bribe and another 12% believe that they lost an opportunity to a competitor that may have paid a bribe. The message is clearly that the war against corruption cannot and should not be limited to the public sector.

Red flags that could identify potential corruption:

- A very short time period given to respond to a tender
- Procurement officials whose lifestyles appear to exceed their income levels
- Orders consistently placed with the same supplier
- Cost of materials out of line when compared with related activities
- Procurement decisions – in favour of key suppliers – that are heavily influenced or made by managers outside the procurement department
- Restrictions in tender documents that have the effect of restricting competition

Responsible people want to work for responsible companies – ones who bring life to their ethical beliefs and "walk the talk"





How is your business strategy aligned with and led by your organisational values?

It is rather easy to point fingers regarding this scourge, but many of the most upstanding and even outspoken members of our society will in certain circumstances be prepared to pay a bribe and thereafter attempt to justify their actions. This is especially the case when their own reputations, or their financial well-being for that matter, are at stake. Consider the businessman who, after having consumed a few glasses of wine at dinner, is stopped by a traffic officer and thinks nothing of trying to buy his way out of this personal predicament. Societal perceptions must be altered and this action should be viewed as no different to the person who requests or pays a bribe to obtain a government tender at an inflated price.

While it is clear that you need two parties to enter into a corrupt arrangement, it only takes one to stop it – a courageous 'NO' in the face of temptation (and often times fear) is all it takes to start paving the path to the end of corruption. The responsibility to stop corruption in South Africa lies with every individual in both the private and public sectors – a decisive stance taken by every element of society in our individual capacities will lead to a revolutionary change to the phrase used too often by many who rationalise this criminal behaviour: 'Everybody's doing it' to 'This is not accepted in our society!'. This is why it is important that businesses must rethink their stance and can no longer lay the blame for corruption in South Africa solely at the door of the public sector – and should never have done so in the first place.

'South Africans have to refuse to accept that corruption is an inevitable way of life.'

Louis Strydom, *PwC Africa Forensic Services Leader*

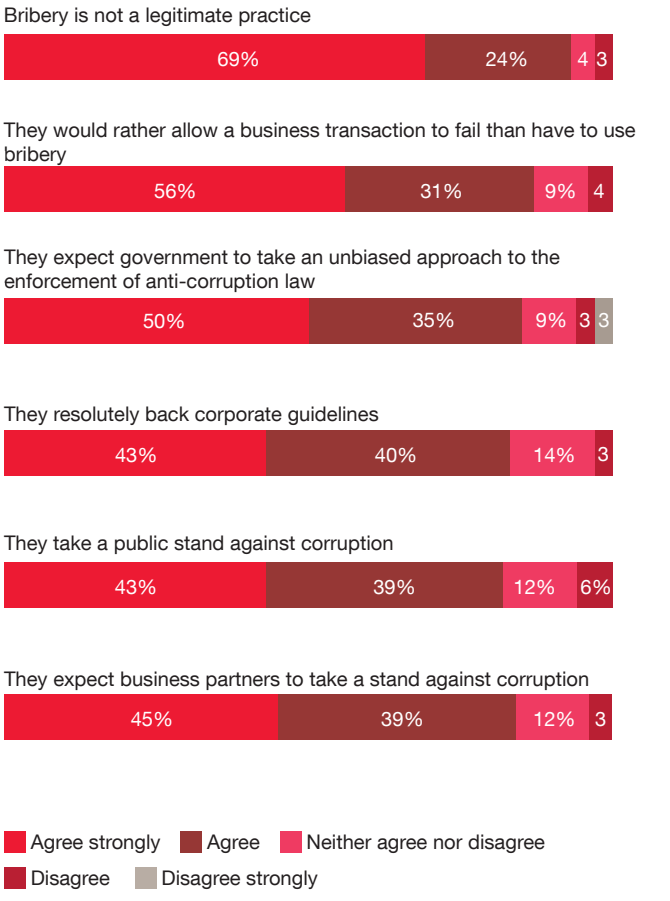
Creating the right environment for compliance

Consider this…

80% of South African respondents indicated that their organisations do have a formal business ethics and compliance programme in place. A similar percentage of our respondents agreed that there are codes of conduct in place that cover key risk areas and govern organisational values and behaviours. This should be good news for a country buckling under the pressure of economic crimes such as corruption – crimes which point to rampant values-based deficiencies – and where almost half of all serious economic crimes in the last 24 months were perpetrated by internal parties. But something does not compute here. If the vast majority of organisations have these programmes in place, why have these not translated into behavioural transformation at an individual level?

When we surveyed the ethical conduct and the proverbial 'tone at the top' of South African organisations, the vast majority of respondents agreed that errant and unethical behaviour were viewed as unacceptable and that corrupt practices in any form, even at the level of views and opinions with regard to these behaviours, were regarded as taboo – and not only do organisations practise and support this stance in-house, they take a public stance against corruption and are active in demanding accountability, even at the doorsteps of government.

Figure 13 How colleagues perceive the way your top level management deals with corruption



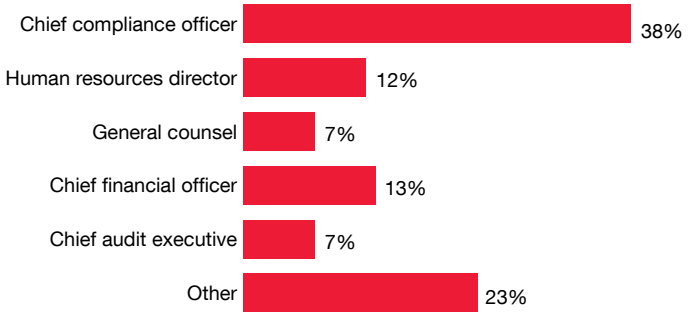
Diving deeper into our statistics, we find that there are signs that perhaps business ethics and compliance are, however, to a large extent theoretical ideas, nice-to-haves that are buried deep inside a filing cabinet, only seeing the light

of day when reviews are conducted or when proposals for business need to be submitted. Our statistics show that only 23% of our respondents could confidently say that training on the code of conduct is provided regularly, supported by regular communications and access to advice channels. This is another sign that there may very well be a divide between what CEOs and boards say and think is happening within their organisations and what's actually happening on the ground. PwC's 19th Annual Global CEO Survey also corroborates this theme of a gap that exists between intention and execution.

This speaks to the need for programmes to not only be in place but be credible in the eyes of all stakeholders. The efficacy of any system, process or programme must be subject to regular testing from an appropriate level and by competent examiners. A large majority (73%) of our respondents indicated that they rely on internal audit to assess the effectiveness of their compliance programmes. Another 41% rely on statutory audit reviews, which are conducted annually. While internal audit is an integral part of the compliance framework, it cannot on its own be relied upon to assure continuous and unfettered compliance. Internal audit, and even more so external audit, by their nature are periodic and post-fact and thus may not be able to keep pace with the rapidly evolving fraud risk profile that companies encounter. Since prevention is ideally placed at the point of decision-making, integrated measures should be preferred. A healthy mix of these elements with reliable management reporting, real-time monitoring, tip-off mechanisms and other measures should form an organisation's core arsenal in preventing and detecting issues in time.

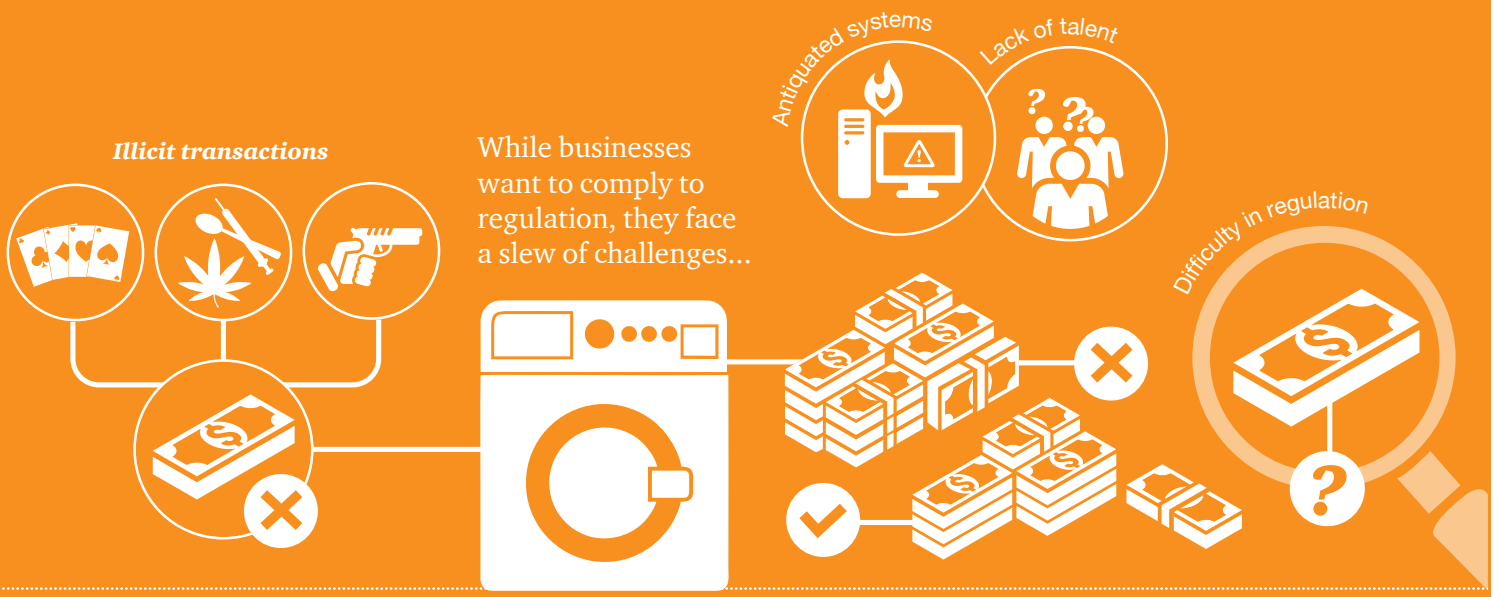
Fostering trust in an organisation and projecting an appropriate tone at the top are key to ensuring that ethics programmes that are in place become living testaments rather than dead scrolls. We noted that of the organisations that had formal business ethics and compliance programmes in place, the responsibility for the programme was very widely dispersed. Having a clear picture of ownership of the programme which is known to all parties within an organisation would alleviate mass confusion and thus provide much needed alignment between corporate ethics and compliance.

Figure 14 Who is responsible for business ethics & compliance programmes?



Compliance spend

Anti-money laundering

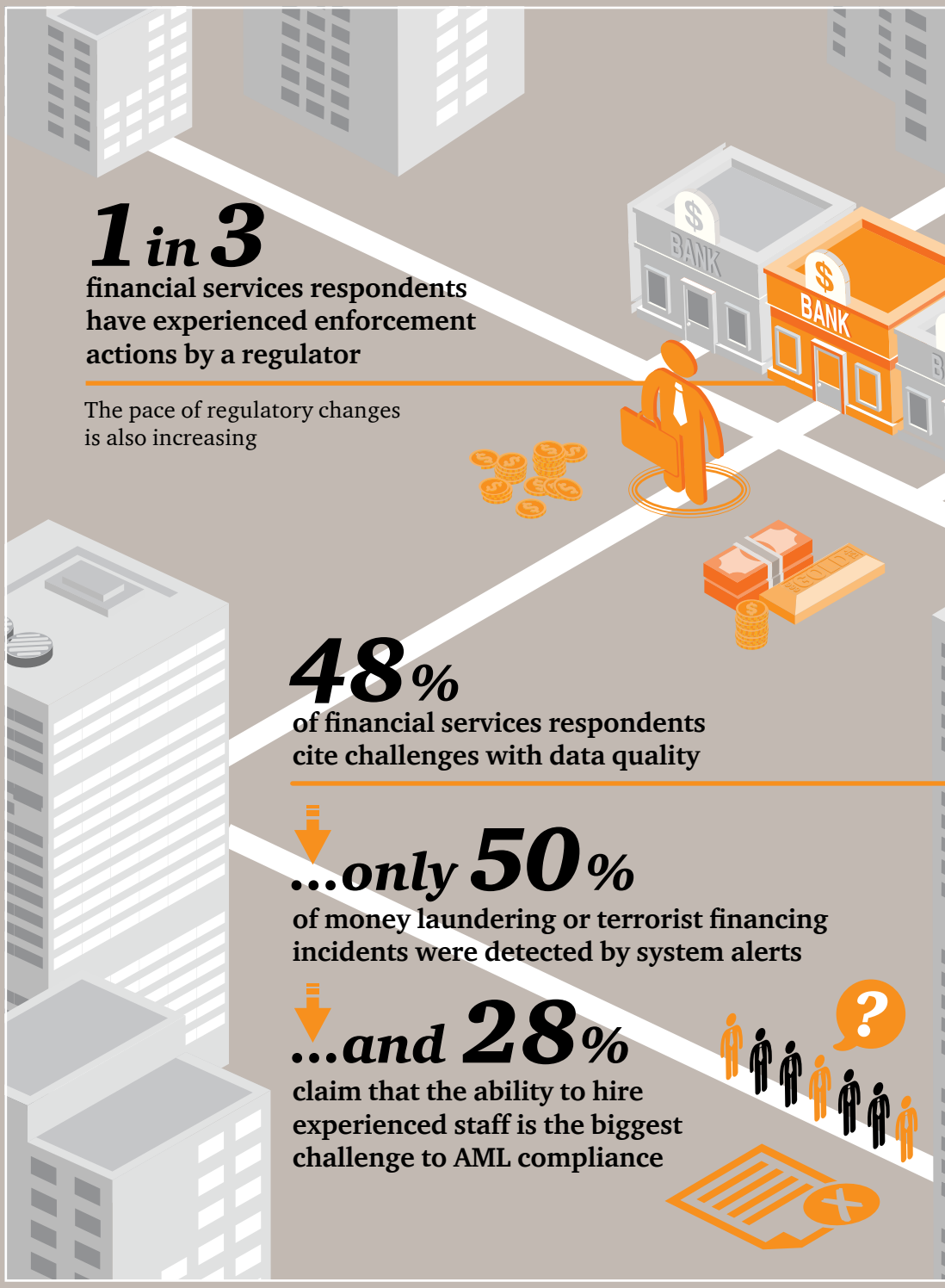


A risk for all seasons

Our global survey makes the bold statement that money laundering destroys value. We can go so far as to say that the impact it has on ethical values is just as damaging, if not more so. We are often faced with the rationalisation of criminal activities by perpetrators of crime, but money laundering takes that to a different level. By cloaking the proceeds from criminal activities so as to hide their illicit origins, money laundering actually facilitates economic crime and nefarious activities such as corruption, terrorism, tax evasion, and even drug and human trafficking. By holding, converting or transferring the funds emanating from these and many other crimes, it inadvertently contributes to the pervasiveness of criminality across the full spectrum (not only economic crime) Thus, any organisation that is (even passively) part of the money laundering cycle faces the risk of not only sustaining damage to its reputation (and bottom line, for that matter), but also becoming an active instrument of the criminal fraternity.

With the rising visibility of terrorist attacks, money laundering and terrorist financing are escalating as priority issues for governments across the globe. Over the last few years, regulators in the United States alone imposed fines in the hundreds of millions to billions of dollars for money laundering and/or sanctions violations. There is mounting pressure across the world, and South African regulators and authorities have already started following suit by taking action against local financial institutions.

Heightened regulatory standards are driving sharp increases in enforcement actions




More than 30%
of financial services firms have not conducted AML/CFT risk assessments across their global footprint
How would your organisation fare in the face of regulatory scrutiny?

Not only banks affected

Traditionally, managing the risks relating to money laundering has been a responsibility squarely on the shoulders of the financial services industry and rightfully so. However, with the changing tides brought about by business integration, the divide between industry sectors is fast disappearing. Any organisation that facilitates financial transactions (and this could very well be every organisation) — including non-bank money services businesses such as digital/mobile payment services, life insurers and retailers, second-hand vehicle dealerships and estate agencies, to name a few — is also coming (and to a large extent is already) within the scope of anti-money laundering (AML) counter financing of terrorism (CFT) legislation in South Africa and, indeed, worldwide.

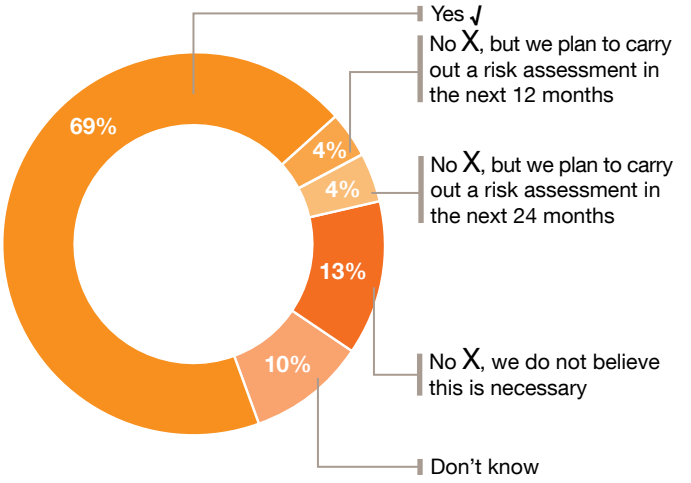
If you carefully peruse the primary South African legislation promulgated to deal with these issues (namely the Financial Intelligence Centre Act, 2001; the Prevention of Organised Crime Act, 1998 and the Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 2004), the building blocks for spreading the net as far and as wide as possible are already in place – but most non-financial organisations are oblivious of the impact this has (or will have) on the way their businesses operate. Not surprisingly, many of these organisations are not up to speed on the requirements and have a tremendous amount of ground to cover if they want to avoid being found wanting from a compliance perspective. Most of the South African organisations surveyed are hesitant to increase their compliance spend; in fact, 40% plan to maintain current (possibly inadequate) levels and a further 4% plan to decrease spend despite the mounting costs witnessed relating to enforcement actions and compliance failures.

Changing tides increase the need for a proactive understanding of risks

Over the last decade, improved money-laundering control measures in the formal financial systems have forced criminals to seek new ways to 'move' the proceeds of their crimes. That's why regular risk assessments are crucial, enabling your organisation to identify and address the money-laundering and terrorist-financing risks you face — wherever and with whomever you do business.

Despite the clear advantages, 31% of the financial services firms in South Africa that participated in our survey either are not currently conducting an AML/CFT risk assessment across their global business footprint or don't know if they are.

Figure 15 Has your organisation performed an AML/CFT risk assessment across its business and geographies?



And as the sophistication of money launderers continues to increase over time, this is a measure that cannot be put off. Trade-based money laundering (TBML), for example — a complex system of false documentation that enables criminals to earn and move value around the world under the guise of legitimate trade — is becoming harder to detect through traditional transaction-monitoring systems.

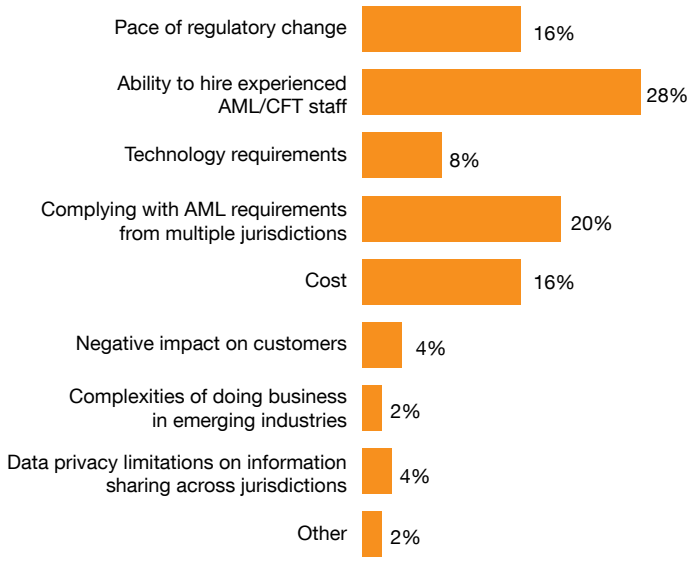
Risk assessments should be conducted on a periodic basis. They should be closely attuned to changed circumstances such as the operating environment, global standards and regulation in countries of operation. Notably, assessments should also include the profiling of customers into different money-laundering and terrorist-financing risk categories. It is also the global standard recommended by FATF and regulators to curb threats.

Common TBML techniques

Can you keep up with the pace of regulatory change?

Worldwide, our survey shows that the level of enforcement of AML and CFT measures has created challenges even for established financial institutions. One in six South African financial services respondents indicated that the pace of regulatory change is a significant challenge to them, and a further 20% feel that way about the 'no-borders' nature of AML compliance.

Figure 16 Most significant challenges to compliance with AML/CFT requirements



This pressure is set to increase even further with the latest wave of fines being imposed — and in some cases, even criminal actions pursued — against financial institutions that have not implemented sufficient controls to monitor their global transactions. Recently, personal liabilities and individual criminal prosecution for custodians of organisations are becoming a more common feature. So, do you really think that you can afford to be complicit?

Expect regulators to be knocking on the door

More than half of our financial services respondents (51%) had undergone inspections by regulatory authorities and no less than two-thirds of them (67%) needed to address major issues and in some cases were placed under an enforced remediation programme.

Institutions that indicated that they have not undergone a regulatory inspection (36%) should expect the proverbial knock on the door. Will you be ready?

AML watchdogs and regulators

- **The Financial Action Task Force on Money laundering (FATF)**, an inter-governmental policy-making and standard-setting body whose current mission is to promote policies to combat money laundering and terrorism financing by monitoring global AML and CFT trends and setting international standards, has established 'Forty Recommendations' — a global minimum standard for an effective anti-money-laundering system, currently adopted by 34 member countries as part of their anti-money-laundering regulation and legislation.
- **The United Nations Security Council** issues resolutions containing inter alia lists of persons against whom sanctions have been imposed, such as known terrorist organisations. These lists are often used by participating governments to support measures against terrorist activity.
- **The Financial Intelligence Centre**, a South African body established by legislation with the aim of combating money laundering and the financing of terrorist and related activities, has the power to impose certain duties on institutions and other persons and, amongst other activities, to provide for the sharing of information by the Centre and supervisory bodies.

What does all of this mean for your company?

With the globalisation of AML/CFT standards, it's important to remember that you may be judged by the highest international compliance standards. Here are three action points to consider:

- **Keep your finger on the regulatory pulse**. Look beyond mechanical compliance with today's laws. Instead, look ahead and examine how to properly structure your organisation to comply with upcoming legislative trends. Focus on having a viable function within the organisation that keeps track of pending regulations in this area.
- **Lead the pack; don't follow**. Being in the middle of the pack exposes you to the risk of falling behind the regulatory curve. Focus on being strategically nimble and innovative to help you stay on top of the regulatory changes.
- **Learn from others' mistakes**. Few organisations are known to actively investigate the root cause of significant issues as identified by regulators. Remediation often serves as a quick solution to address regulatory findings — yet the cost of remediating breaches often outweighs penalties imposed by regulators. Since most transactions have a multinational financial component, it is good practice to default to the highest global standard of compliance whenever possible, and to undergo more rigorous AML/CFT self-assessments. Establish 'enterprise-wide' requirements to ensure consistency across geographies.

Regulation by examination

A further challenge for organisations wrestling with global AML/CFT compliance is that regulatory expectations are increasingly replacing clear legal requirements (especially in customer due diligence and transaction monitoring). Examiners may apply a standard on one institution based on the practices of another. This so-called 'regulation by examination' challenges the well-known risk-based approach concept that organisations and their stakeholders are expected to apply.

The people challenge

Hiring the right calibre of personnel with the requisite experience is the most significant issue facing South African financial services institutions, with 28% of our respondents citing this problem. This issue will no doubt be amplified significantly with non-FS counterparts that have not really cut their teeth on the AML issues.

This translates into the fact that the supply of talent (which is already under strain) will continue to fall behind rising demand. Consequently, churn among AML and compliance staff is high, and competition for top-shelf people is significant for both financial services and non-financial services companies.

More than half of our respondents are addressing the talent challenge through training of in-house resources, with a significant focus on both AML/CFT and anti-bribery resources, and 53% sought to hire additional resources with the requisite talent to fill specific roles.

Figure 17 What people measures has your institution implemented in the last 24 months to address increased regulatory expectations?

Right people, right skills, right places. What skills do you need?

When your best line of AML defence is having the right people with the right skills in the right roles, you need to know what you are looking for. There's significant demand for specialised expertise and skills around:

- Global standards and requirements
- Jurisdictional regulations and obligations
- The global regulatory ecosystem
- Customer due diligence
- Technical expertise in transaction monitoring
- Data analytics

Participation statistics

Respondents

232
South African respondents

84%
of respondents in Executive Management, Finance, Audit, Compliance or Risk Management

35%
of the survey respondents represented publicly traded companies

50%
of respondents were from multinational organisations

Industry sectors

28% Financial Services

26% Industrial

17% Government & State-owned

10% Consumer

5% Agriculture

14% Other

Contacts

Africa Forensic Services Leader

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

Forensic Investigations & Litigation Support

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

Lionel van Tonder
Partner, Pretoria
+27 12 429 0400
lionel.tonder@za.pwc.com

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

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

Ettienne Lambrechts
Associate Director, Pretoria
+27 12 429 0061
ettienne.lambrechts@za.pwc.com

Frans Lekubo
Associate Director, Johannesburg
+27 11 797 5867
frans.lekubo@za.pwc.com

Anti-bribery and Corruption

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

Expert Accounting & Dispute Resolution

Colm Tonge
Partner, Johannesburg
+27 11 797 4007
colm.tonge@za.pwc.com

Gerhard Sohnge
Associate Director, Johannesburg
+27 11 797 4859
gerhard.sohnge@za.pwc.com

Corporate Intelligence

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

Cybercrime & Forensic Technology Services

Junaid Amra
Associate Director, Durban
+27 31 271 2302
junaid.amra@za.pwc.com

Fraud Prevention Consulting

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

Anti-Money Laundering

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

Survey management team

Moazam Fakey
Senior Manager, Johannesburg
+27 11 797 4750
moazam.fakey@za.pwc.com

Rolindi Devenish
Manager, Pretoria
+27 12 429 0385
rolindi.devenish@za.pwc.com

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

Data resources

Looking for more data?

The crime survey website www.pwc.co.za/crimesurvey has been designed to be an extension of the survey with many exciting and useful resources for readers wishing to delve deeper into the data, including:

- Survey methodology
- Terminology
- Comparative country counts
- Additional information regarding the nature of participants

In addition, this year's survey data has been loaded onto an innovative tool referred to as the Global Data Explorer which will allow visitors to the site the ability to customise their analysis of the data for their specific needs.


CaTSH Network
CU MPLS
Beijing
Fortune Plaza
Beijing
Prosper Center
Shanghai
PwC Center
Shanghai
Shui On Plaza
Hong Kong PB
Singapore
Internet

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.

© 2016 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. (16-118353)