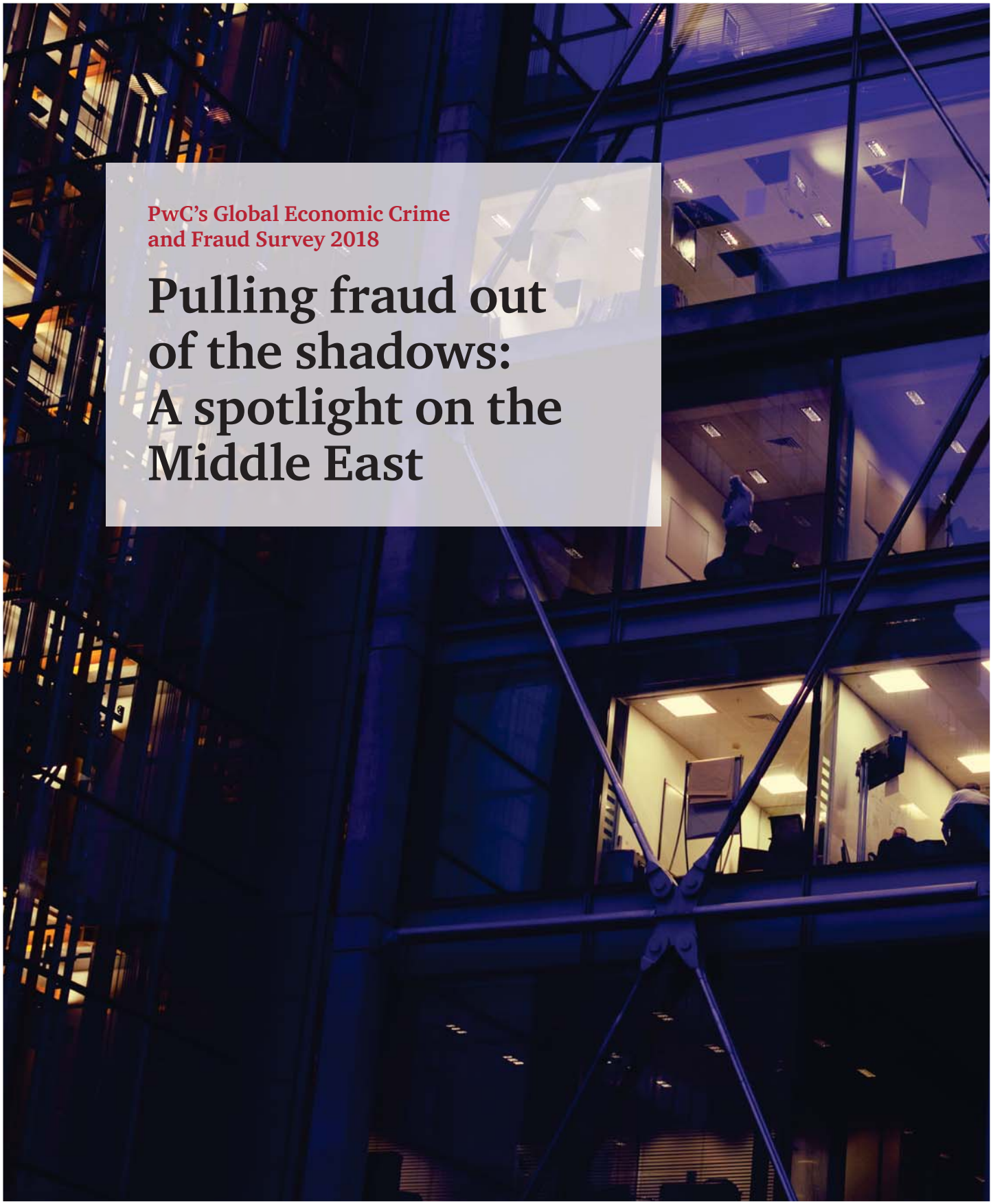


PwC's Global Economic Crime and Fraud Survey 2018

Pulling fraud out of the shadows: A spotlight on the Middle East

pwc

www.pwc.com/me/crimeandfraudsurvey

Fraud, the biggest competitor you didn't know you had

PwC's Middle East Economic Crime and Fraud Survey 2018 confirms that economic crime is maintaining its trajectory in the region and continuing to disrupt businesses.

Nick Robinson
Middle East
Forensics Leader

Tareq Haddad
Middle East
Investigations Leader

Current results follow established historical trends, with the proportion of organisations reporting that they've fallen victim to acts of fraud and economic crime increasing to 34%, up from 26% in 2016. While this rise could be attributable to an increase in awareness of economic crime and an improvement in detection mechanisms within organisations, what we should really be asking is: "What about the other 66% of organisations lurking in the shadows?"

This question is essentially about the amount of fraud that's still going unseen or unreported. And it's given greater urgency by the fact that two new categories of fraud that were only introduced into the survey this year – business misconduct and fraud committed by consumers – emerged as the most reported crimes experienced by organisations across the region.

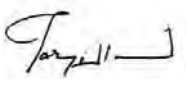
Each of us has personal experience of the ever-expanding part played by technology in all aspects of our lives, and of its evolving role in fraud prevention and cyber intrusion in the work environment. The stakes are increasing in tandem as technology affords perpetrators the ease and convenience of being able to cause disruption from the comfort of their living-rooms. However, the impact of technology also works the other way, with companies moving to take control and leverage technology to help fight and prevent crime in the workplace.

Alongside the growing role of technology, the survey results strongly underline the importance of people, confirming that people can be both your greatest ally and your strongest foe in the fight against fraud. By investing in your people it will not only help prevent crime – but will also motivate and push economic growth in your workplace forward.

In addition to highlighting and analysing the visible frauds that organisations are facing, this report also outlines steps to knowing your business better, illuminating the blind spots of economic crime lurking in the shadows. By doing this, we hope our study will enable you to see the bigger picture – and equip yourself and your business to actively tackle fraud risks head on, emerging stronger as a result.

We would like to extend our thanks to all of the organisations and respondents who made the 2018 Middle East Global Economic Crime and Fraud Survey possible.

Nick Robinson



Tareq Haddad

Contents

Leading Observations

Economic crime is being pulled out of the shadows

More organisations reported experiencing fraud in the Middle East in the past 24 months. The proportion increased to

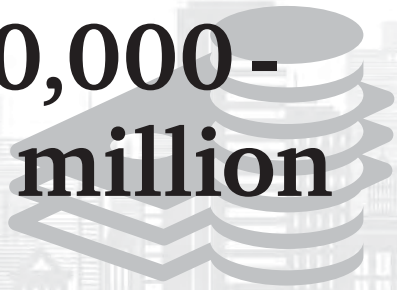
34% from **26%**

Economic threats are evolving. Two new categories of fraud introduced to the study this year – namely

have emerged as the economic crimes most often reported, alongside asset misappropriation.

The most disruptive economic crime experienced by organisations has cost

46% of respondents between **US$100,000 - US$50 million**



Is this consistent with the fraud trends you are seeing in your organisation – and how can you take action in response?

Technology is proving to be a strong ally

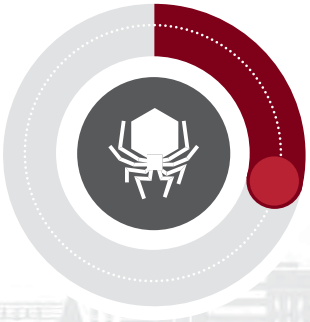
Reliance on technology is on the rise, with

52%

of organisations using technology as the primary monitoring technique for fraud and economic crime in relation to cyber-attacks and vulnerabilities.

82% of respondents agree that the use of continuous real-time monitoring assists their organisation in combating economic crime.

77% of organisations have a response plan to deal with cyber-attacks, a significant rise from 33% in 2016.



29% of organisations think that cybercrime is likely to be the most disruptive crime in the next 24 months.

Is your organisation part of the move towards greater use of technology, or are you at risk?

Leading Observations

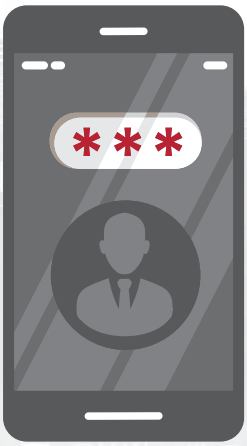
People are key

Internal fraud actors are increasingly active, accounting for **48%** of the most disruptive economic crime experienced.

Abuse of trust and resources is prevalent, with **62%** of reported internal fraud being attributed to senior and middle management as the main perpetrators.

One in ten respondents have been asked to pay a bribe in their home country.

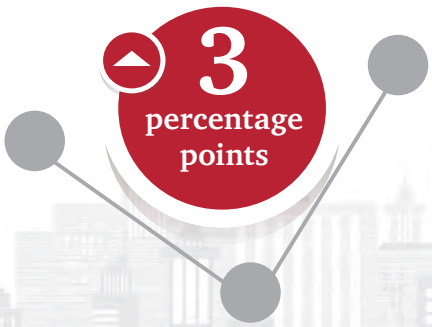
Of the three highest reported types of economic crime, fraud committed by consumers is the leading disruption faced by organisations.



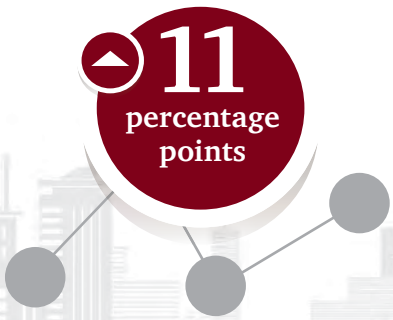
Are your awareness programmes targeting the culture of your organisation and region?

The traction of detection of fraud and economic crime is growing

Routine internal audits are the leading means of fraud detection in organisations.



Formal business ethics and compliance programmes are gaining strength, with the proportion of organisations that have programmes increasing by 3 percentage points to 82%.



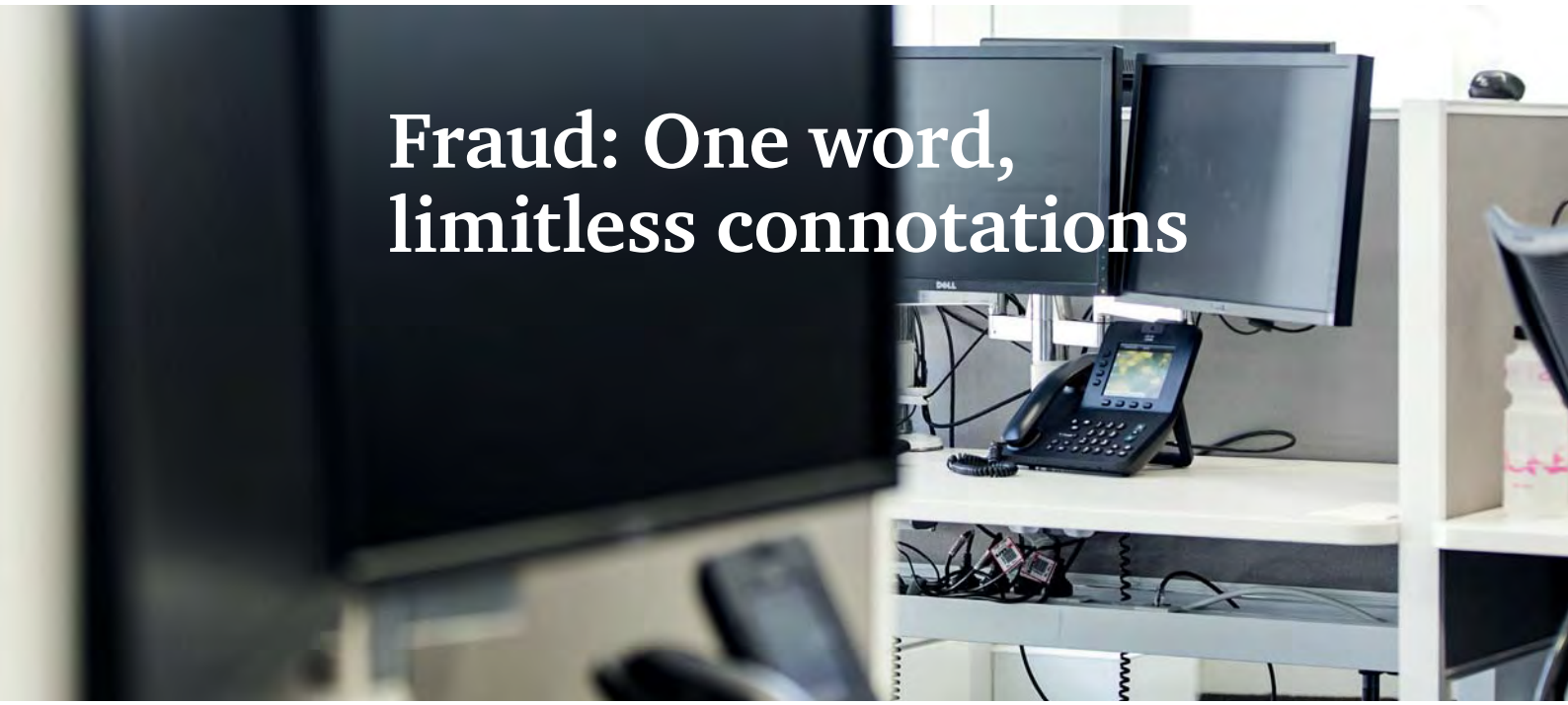
Trust and confidence are key: in the past 24 months there has been an increase of 11 percentage points in the reported rate of internal tip-offs, which represents the second most common means of detecting fraud.

The proportion of organisations that have performed a risk assessment at least once within the past 24 months has risen to over **77%**

This is marginally higher than the global average.

How much fraud are you detecting – and are you adequately prepared?

Fraud: One word, limitless connotations



34%

of organisations reported they've experienced fraud in the last 24 months

Source: PwC's Global Economic Crime and Fraud Survey 2018: Middle East Spotlight

For almost two decades, PwC has been monitoring global trends in fraud and economic crime and for at least a decade has been generating reports specifically for the Middle East region. In our Global Economic Crime and Fraud Survey 2018: Middle East Spotlight report, we surveyed 146 respondents from 10 different countries throughout the Middle East.

At a headline level, the findings confirm that reported economic crime in the region remains on the increase, with one in every three organisations reporting that they have been a victim of economic crime – up from 26% to 34% in the past 24 months.

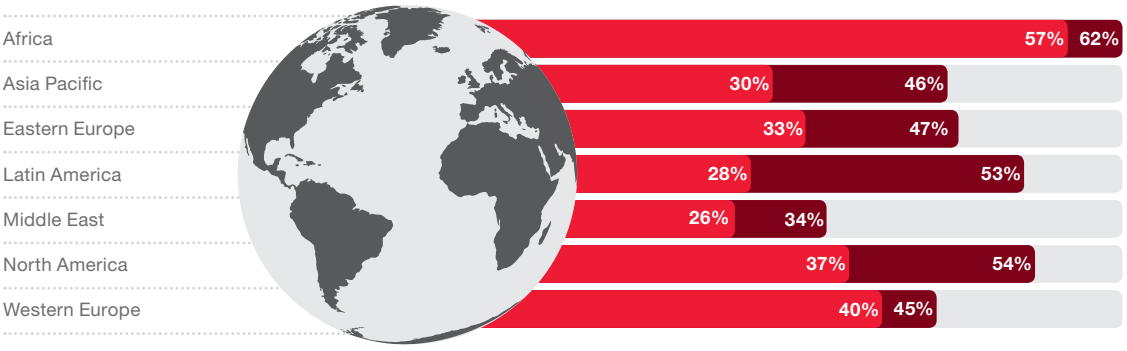
Despite the rise, this figure is still well below the global finding of 49% of organisations reporting they've experienced fraud, and also less than the levels of reported crime in other regions of the world. However, the Middle East does mirror the rest of the world in seeing a significant increase in reported economic crime. So, what's happening? Is fraud really on the rise, both globally and in the Middle East, or is it that our awareness of fraud is increasing?

The harder you look, the more you find…

The plain answer is that it's hard to tell. What is clear is that the rise in reporting of incidents of fraud at both a global and regional level is being fuelled by increasing awareness and scrutiny of economic crime risks among all stakeholders – including businesses, employees and the general public. Also, this dramatic rise in awareness is in turn helping to trigger regulatory action to bear down on fraud, with the effect of intensifying organisations' scrutiny of this area still further.

The region's increasing focus on fraud is reflected in rising spending on efforts to tackle it: 42% of Middle East organisations in our study have reportedly increased the amount of money allocated to combating fraud and economic crime within the past 24 months, the same proportion as at a global level. And 49% plan to increase it in the next 24 months, ahead of the global figure of 44% – indicating that the focus on fraud is set to rise more quickly in the Middle East than elsewhere.

Figure 1: The reported rate of economic crime has increased across all territories



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

Source: PwC's Global Economic Crime and Fraud Survey 2018: Middle East Spotlight

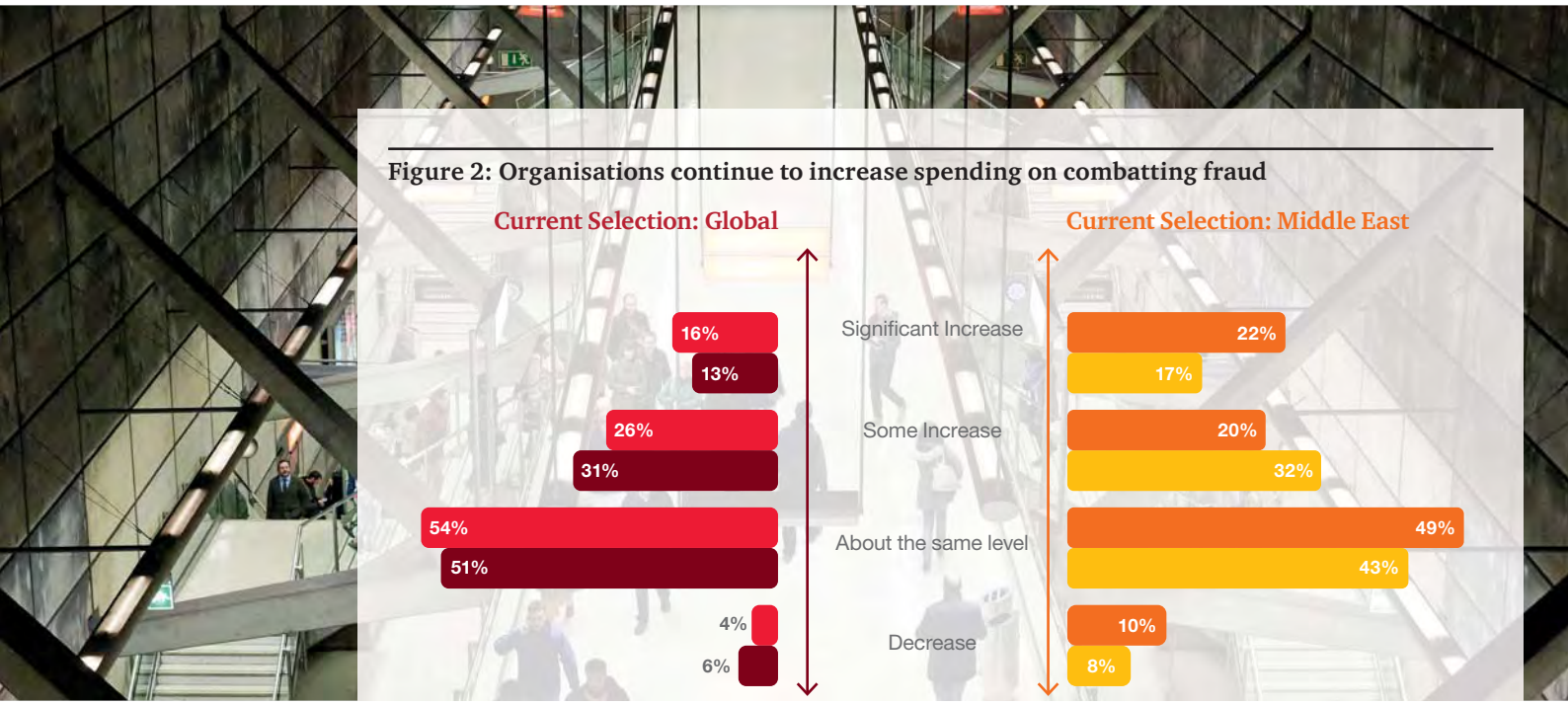
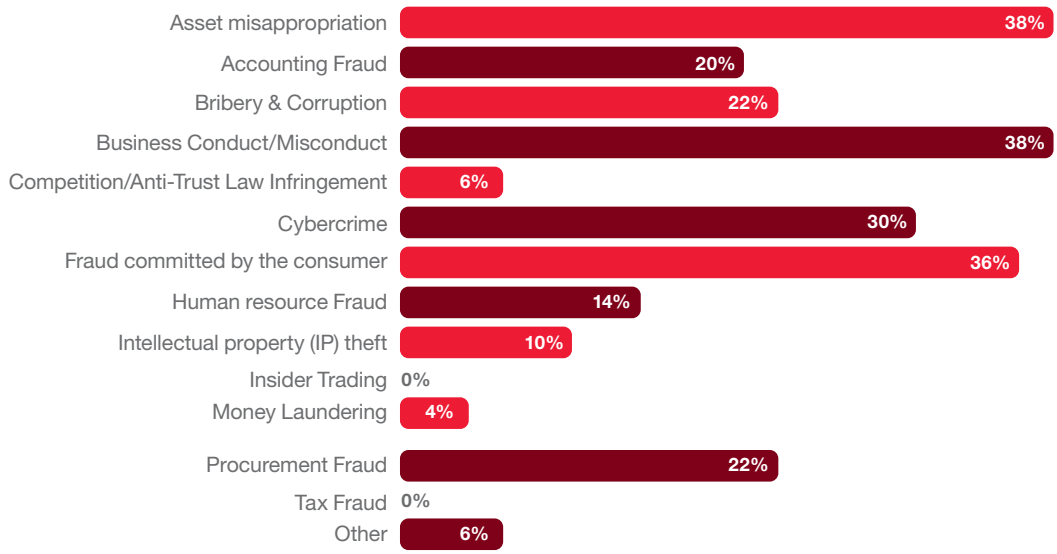


Figure 2: Organisations continue to increase spending on combatting fraud

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

Source: PwC's Global Economic Crime and Fraud Survey 2018: Middle East Spotlight

Figure 3: Types of economic crime/fraud experienced



Source: PwC's Global Economic Crime and Fraud Survey 2018: Middle East Spotlight

Tax fraud: a crime whose time may have come

As we've pointed out, fraud is a single word with many connotations. But one connotation it hasn't carried to date in the Middle East is around tax, with our respondents in the region reporting no instances of tax fraud over the past 24 months.

However, this may well be about to change, with the recent imposition of VAT in certain GCC countries transforming the potential for tax fraud, and creating an urgent need for preventative action.

60%

of respondents in the region believe that changes in the geopolitical environment will impact the regulatory environment

Source: PwC's Global Economic Crime and Fraud Survey 2018: Middle East Spotlight

Formal business ethics and compliance programmes continue to see increased investment in the Middle East

…as region-specific factors come into play

This increasing commitment to identifying and addressing fraudulent behaviour is being fostered by developments at a regional level. Reflecting the Middle East's pivotal strategic and geographic position and role in the world, some 60% of respondents in the region believe that changes in the geopolitical environment will impact the regulatory environment – and almost half think they will bring change to enforcement regulations. It further appears that geopolitical shifts are encouraging respondents to increase their resources on fighting fraud.

At the same time, developments in the interface between governments and the commercial sector – including growing efforts to attract international capital into the region's businesses, and rising use of public-private partnership (PPP) structures for infrastructure funding – are boosting awareness of the need to align with international standards of governance and compliance. Significantly, formal business ethics and compliance programmes continue to see investment in the Middle East, with the proportion of organisations that have these programmes rising by 3 percentage points. This is in stark contrast to a 5 percentage point decline in the proportion of organisations that have these programmes in place globally.

Counting the cost of fraud – both financial and in terms of damage to morale

In terms of the cost of fraud to organisations, the financial impacts are clearly substantial: the most disruptive economic crime suffered over the past 24 months has cost 46% of respondent organisations between US$100,000 - US$50 million dollars. Equally alarmingly, these impacts are not always communicated to the people at the top. In 4% of cases, the most disruptive fraud incidents identified in the organisation are not reported to the board, and in 8% the respondent did not know if these were reported.

Types of economic crime: the customer isn't always right…

Turning to the types of economic crime that organisations are encountering, the three most common forms of fraud reported in the region are asset misappropriation, business misconduct and consumer fraud. This differs from the top three economic crimes at a global level, where cybercrime ranks second behind asset misappropriation and ahead of fraud by consumers. Within the region, the rising impact of fraud by consumers is a significant feature of our findings, with respondents citing it as the leading source of disruption within the top three types of fraud.

Figure 4: The most common forms of fraud reported by Middle East respondents

Source: PwC's Global Economic Crime and Fraud Survey 2018: Middle East Spotlight

Corruption is a key link to the fraud chain

A further characteristic of the Middle East fraud landscape that emerges from our study is the close link between corruption and fraud. Business misconduct fraud is an emerging threat with, globally, 28% of fraud victims saying they have experienced it in the past two years. But it's especially prevalent in the Middle East, with a response rate of 38%.

It is often the case that people do not pay bribes with their own money which implies that there is a fraud cycle of illicit funds being churned.

Our research underlines that, in the Middle East, 10% of respondents have been asked to pay a bribe in their countries and 7% have been asked to pay a bribe outside of their countries with the respective global comparatives of 17% and 9%. Furthermore, one in every ten respondents in the region believe they have lost an opportunity to a competitor who paid a bribe in the country they primarily work in and 8% out of their country.

It is also worth mentioning that every two in three companies in the Middle East specifically use ethics and compliance programs to help them combat anti-corruption and anti-trust programmes risks.

10%

of respondents have been asked to pay a bribe in their countries and 7% have been asked to pay a bribe outside of their countries

Source: PwC's Global Economic Crime and Fraud Survey 2018: Middle East Spotlight

AML: A cross border regulation

Our survey highlights that AML regulations are crossing borders where out of the respondents involved in moving money, 54% are subject to both local and other countries' AML regulations and 7% are subject to only other countries' regulations.

Anti-money laundering/counter-terrorist financing (AML/CFT) monitoring has traditionally been a high priority for organisations across the Middle East. With 24% of the respondents from the financial services industry, our study shows that the proportion of organisations undertaking AML/CFT risk assessments has fallen by 12 percentage points in the past 24 months, with only 67% of organisations performing one. Half of this can be attributed to the rising percentage of respondents who are unaware if their organisation undertakes an AML/CFT risk assessment.

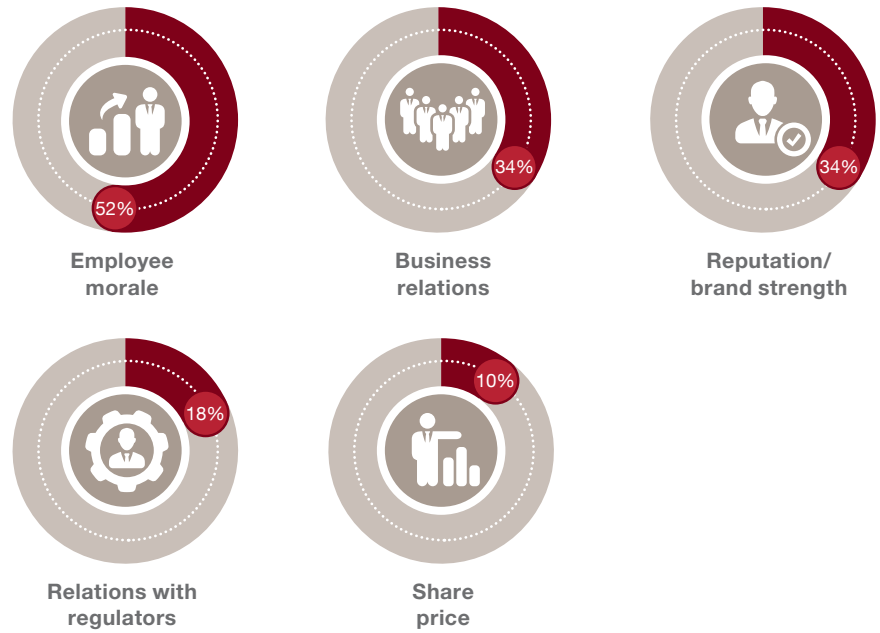
Unless organisations undertake an adequate assessment of the risks, they will be ill-prepared to respond to incidences of financial crime and ensure they are investing money into appropriate controls. The need for such assessments is underlined by the fact that 23% of respondents have either undergone an enforced remediation programme or received major feedback from a regulatory inspection. This evidences the global trend towards regulators taking a tougher stance on organisations that fail to adequately mitigate financial crime risks.

Intangible costs outweigh the financial costs suffered by organisations

However, the biggest perceived impacts of fraud are not financial, but through their damaging effects on people's wellbeing and perceptions.

Employee morale is cited as the leading side-effect of crime in the workplace, while the second highest negative impact is the effect on public perception. While these findings are echoed in the global context, it is clear that organisations in the Middle East are taking notice of the effects of fraud on the people within and beyond the business.

Figure 5: Fraud and economic crime impact many aspects of organisations in the Middle East



■ High to medium

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

Source: PwC's Global Economic Crime and Fraud Survey 2018: Middle East Spotlight

Harness the protective power of technology

29%

of organisations think cybercrime is likely to be the most disruptive crime in the next 24 months

Source: PwC's Global Economic Crime and Fraud Survey 2018: Middle East Spotlight

Cyber threats continue to grow…

One of the most striking – and worrying – findings from our study is that only 50% of the respondent organisations in the Middle East have performed a cyber-related risk and vulnerability assessment in the past 24 months. Given this relatively low level of vigilance, it's sadly unsurprising that at least 59% have been targeted by cybercrime during the same period.

As in previous years, most of these crimes have been perpetrated through phishing and malware attacks – a trend that has made anti-malware solutions deployment, systems patching, user education and awareness key priorities for countering cyber crime strategies. At the same time, the vital importance of tackling cyber risks is underlined by the disruptive impact of attacks when they occur: 22% of respondents who have experienced fraud cite cybercrime as their most disruptive incident, and 29% of organisations think cybercrime is likely to be the most disruptive crime in the next 24 months.

In terms of the form of cyber crime, the region-wide move towards digital and always-on service provisioning means the biggest impact of cyber attacks usually springs from its disruptive effect on business processes. From the criminal's viewpoint, this is part of the attraction of cyberattacks, providing an easier way to cause disruption than alternative methods such as extortion, misappropriation and procurement fraud, all of which require more sophisticated attack procedures.

Looking to the future, it seems highly likely that the number of organisations targeted by cyber criminals will continue to grow across all the categories of attack. We also expect extortion, misappropriation and procurement fraud to keep growing, thanks to the new vulnerabilities introduced by relatively less mature digital solutions and increased usage of automation.

…but organisations are rising to the challenge

Having said all that, there are some more encouraging findings from our research. Most positively, 77% of organisations now have a response plan in place for dealing with cyberattacks (up from just 33% in 2016), and most of them are likely to share information with government and law enforcement agencies, making the region more resilient in the future. Due to the rising probability and potential impact of cyber attacks, we expect most of the remaining large and medium-sized enterprises and government entities to have a response plan (and potentially to exercise it) in the coming few months.

Using technology to enhance fraud detection

82%

of respondents in the Middle East agree that continuous real-time monitoring assists their organisation in combating fraud

Source: PwC's Global Economic Crime and Fraud Survey 2018: Middle East Spotlight

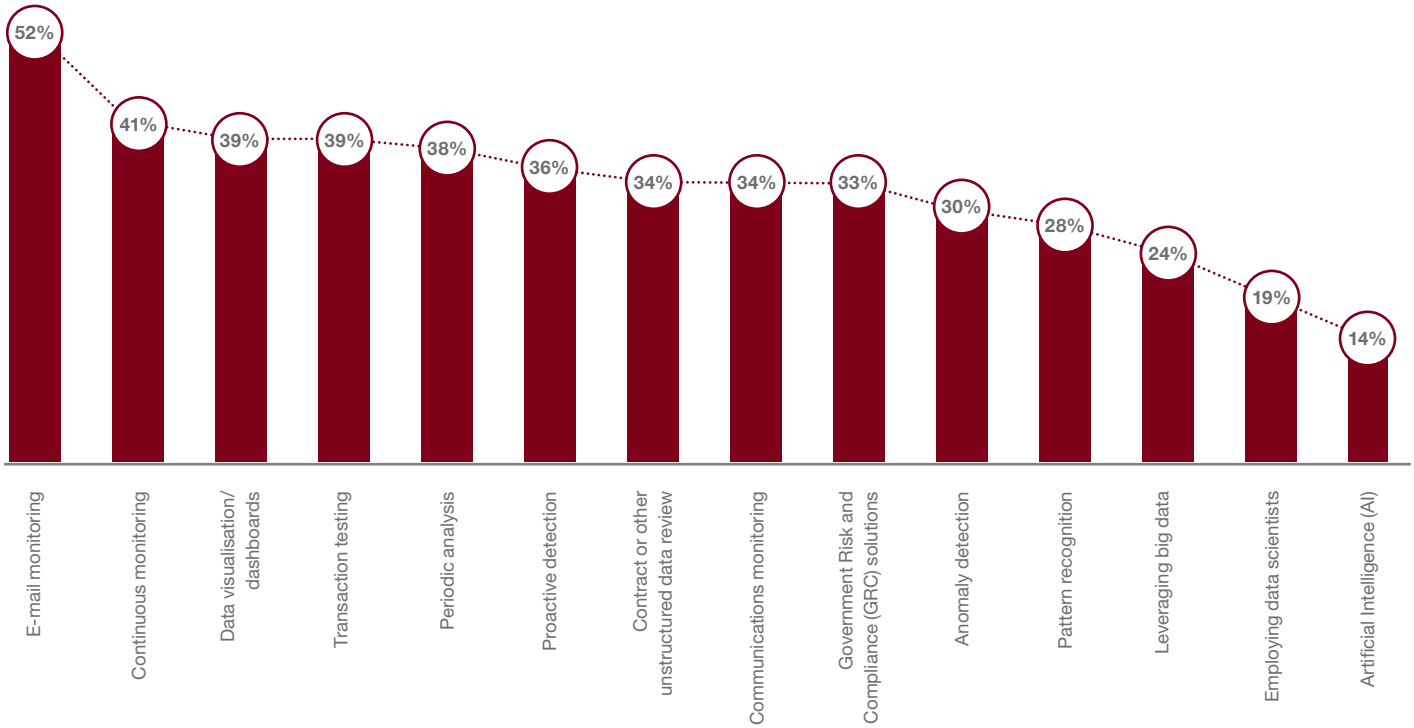
Keeping your hand on your pulse

Despite the challenges we've described, organisations are realising rising value from anti-fraud technologies, and are looking to extend their usage of it. Some 82% of respondents in the Middle East agree that continuous real-time monitoring assists their organisation in combating fraud.

Email monitoring is on the rise

Email monitoring is relatively simpler to implement than real-time monitoring, and our study finds that half of organisations in the region are already using or considering using it to help them combat fraud. Looking forward, a combination of rising interest among organisations and increasing activity from vendors means most large and medium-sized enterprises and government entities will look towards using email monitoring within the next 12 to 18 months.

Figure 6: Organisations are beginning to derive value from alternative and disruptive technologies in combatting fraud



Q. To what degree is your organisation using and finding value from the following alternative/disruptive technologies and techniques in your control environment to help combat fraud and/or economic crime? (% of respondents who said their organisation uses and derives value)

Source: PwC's Global Economic Crime and Fraud Survey 2018: Middle East Spotlight

Organisations in the Middle East are making growing use of technology in their anti-fraud efforts, with 52% saying they rely on technology as their primary monitoring technique for detecting fraud

The fact that around half of our Middle East respondents are either using or considering email monitoring to tackle fraud, reflects the continuing strong role that email plays in many commercial transactions in the region.

The email monitoring being deployed comes in various forms. Approaches range from monitoring email traffic continuously and in real time, to more selective monitoring focused on particular time periods or higher-risk areas. By combining email monitoring with artificial intelligence and visualisation software, organisations can analyse suspicious activities and identify breaches much more quickly.

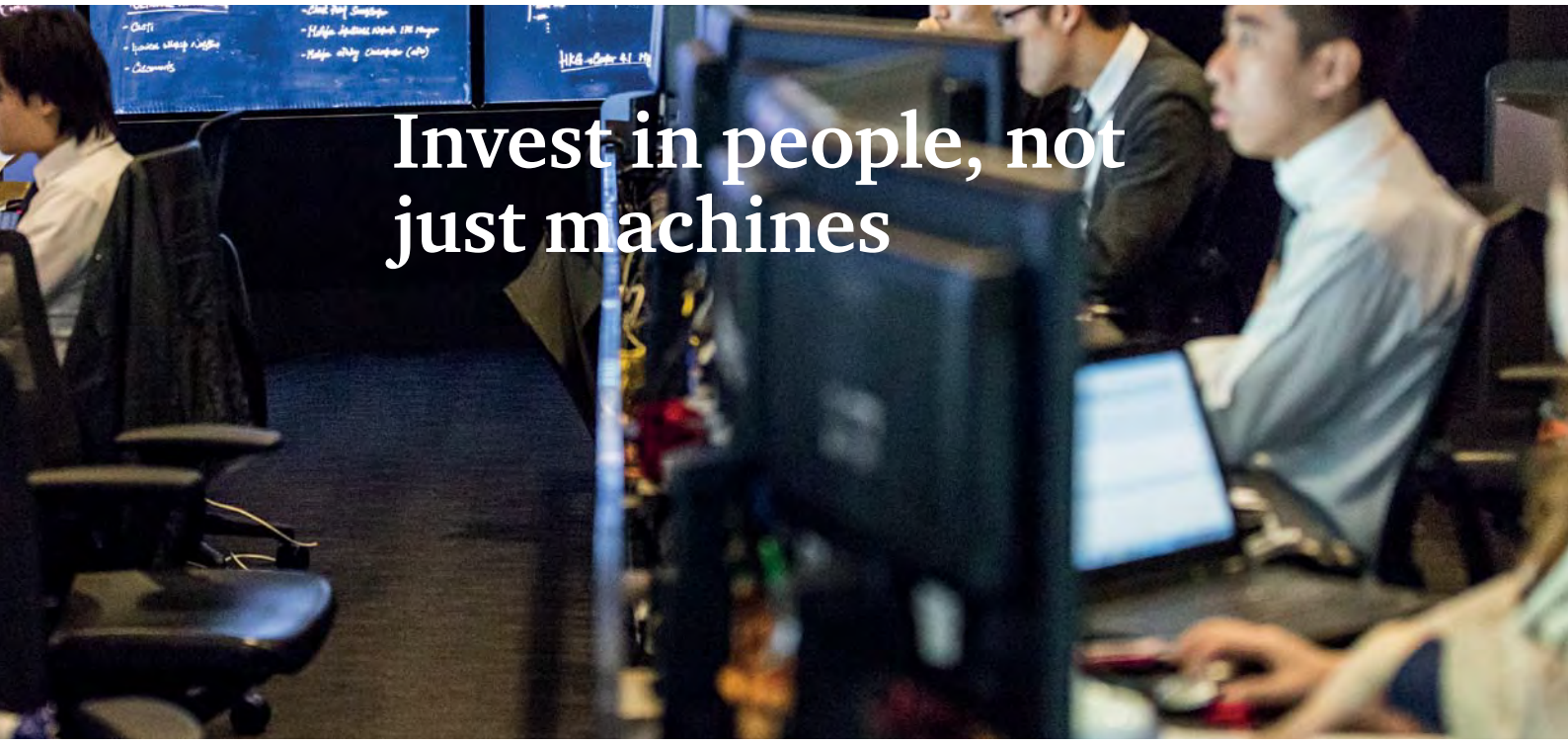
Data on employees' communications – including internal email and chat – can also be used for sentiment analysis, identifying trends in their behaviour, stress levels and working relationships. And technologies like natural language processing and machine learning can help management predict issues that could lead to crime or misconduct, and address any nascent dissatisfaction before it spreads and disrupts the business.

Artificial Intelligence (AI): An ally you didn't know about

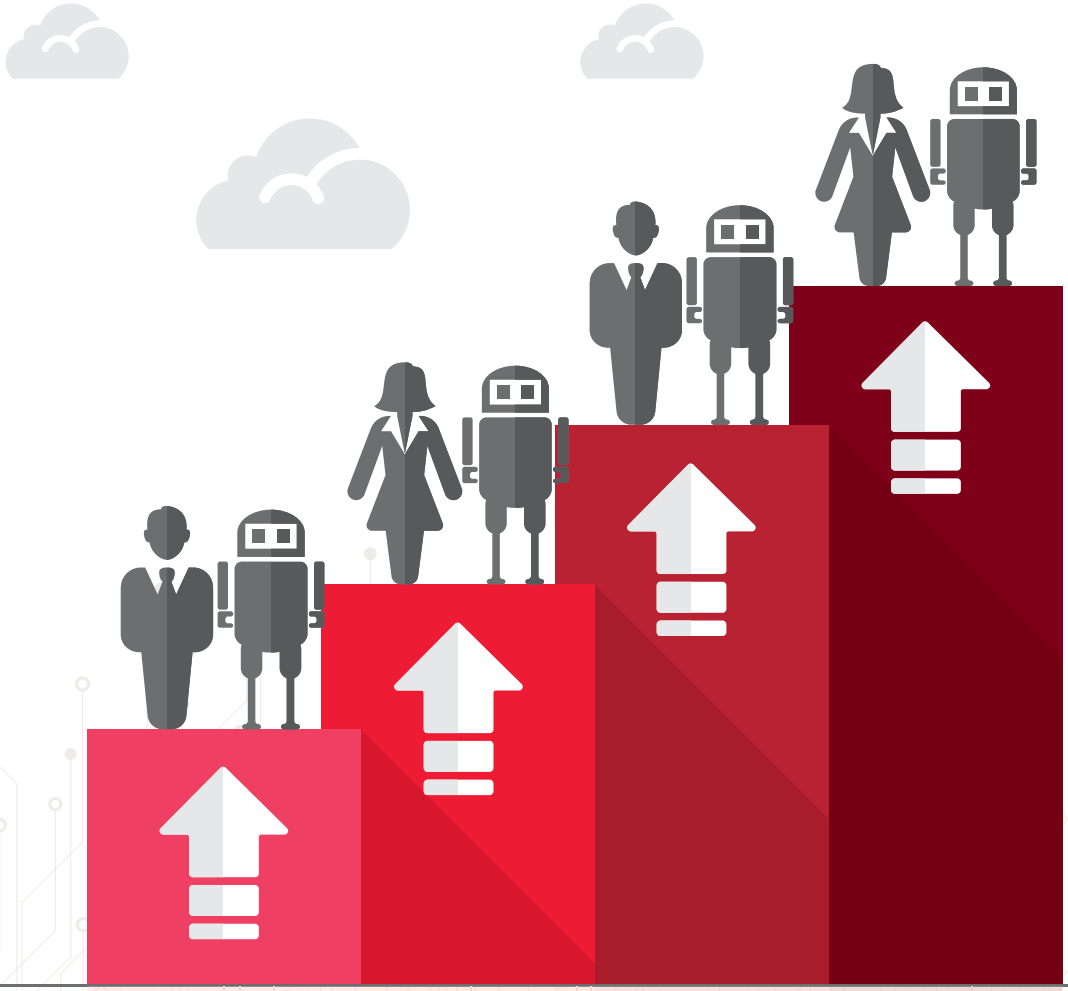
Organisations in the Middle East are making growing use of technology in their anti-fraud efforts, with 52% saying they rely on technology as their primary monitoring technique for detecting fraud and economic crime in relation to cyber-attacks and vulnerabilities. But there are limits to this usage, with only one-third of respondents reporting that their organisations are taking advantage of AI to help detect fraud. Amplifying human intelligence with AI in the workplace has the potential to take many organisations' fraud detection to new heights.

That said, a global comparison suggests that Middle East organisations' rate of AI adoption for anti-fraud purposes is relative. In our global study, 27% of companies in developing territories said they currently use or plan to implement AI to combat fraud, while just 22% of companies in developed territories said the same. Set against such findings, the one-third of Middle East organisations using AI is impressive.

One potential issue that organisations must be wary of in using AI for fraud detection is data integrity. The region has recently seen a decade-long period of accelerated economic activity, driving a growth surge with which many organisations' systems have struggled to keep pace. Amid this expansion, data integrity is an area that's often been given too little focus. Organisations need to ensure their data is robust, timely and accurate before layering new anti-fraud systems and AI on top.



Invest in people, not just machines



11%

the rise in internal tip-offs over the past 24 months, making it the second highest means of fraud detection

Source: PwC's Global Economic Crime and Fraud Survey 2018: Middle East Spotlight

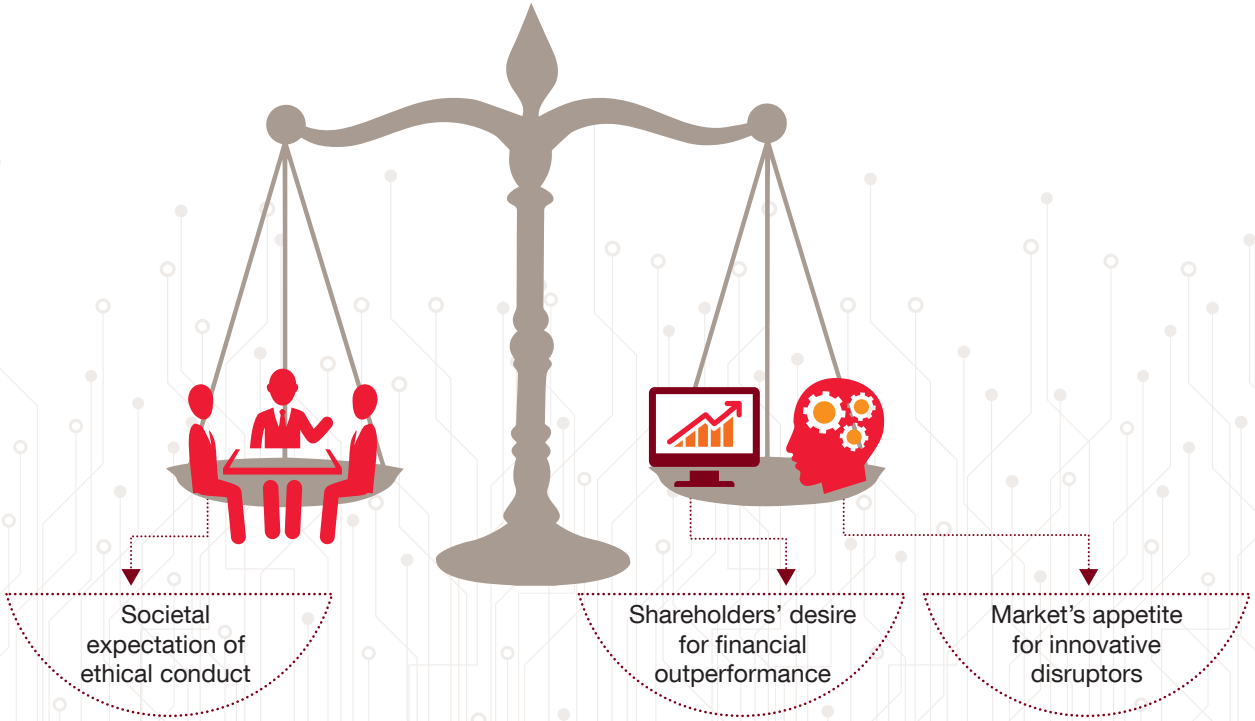
Investment in people will yield your greatest returns yet

While technology is playing a growing role in tackling fraud in organisations, it is important to understand that it isn't the answer on its own – and that it is even more vital to focus on the people behind the technology. This means carrying out regular assessments of fraud risks, that considers factors relating to human aspects, and keeping a close eye on factors such as incentives that might encourage fraud.

A common misconception facing many organisations is that the responsibility of combating fraud is side-lined to a specific function. A clear message to be reinforced is that fraud detection is a collective responsibility. Detecting, preventing and dealing with economic crime is everybody's job, which in turn impacts the wellbeing of the organisation and everyone in it, an example thereof is the reputation of the organisation. Implementing a pervasive culture of vigilance and zero tolerance for fraud risks helps everyone understand that fraud is never "someone else's problem".

The vital importance of people in combating fraud is underlined by the fact that routine internal audits are leading the pack as the fraud detectors in organisations across the region, accounting for the biggest share of crimes uncovered.

Also, the report rate of internal tip-offs has leapt by 11% in the past 24 months, making it the second highest means of fraud detection – a finding that underlines the importance of employee trust, engagement and confidence in addressing fraud. So while usage of detection techniques such as automated email monitoring are growing strongly, traditional people-based methods continue to dominate.



48%

of Middle East respondents say that an internal actor was responsible for the most disruptive fraud experienced

Source: PwC's Global Economic Crime and Fraud Survey 2018: Middle East Spotlight

Putting a face to the fraudster

The profile of the people committing economic crime in the Middle East continues to evolve, providing organisations with useful pointers for combatting it. The proportion of fraud instigated by internal fraud actors is increasing rapidly, accounting for 48% of economic crimes reported by respondents, slightly below the global average of 52%.

With abuse of trust and resources emerging as common forms of wrongdoing, senior and middle management are the main perpetrators of internal frauds, accounting for 62% of those reported. Our study also shows that one-third of fraudsters work in the operations or production functions.

External threats are also on the increase in the Middle East. Fraud actors from outside the organisation committed 41% of reported incidents – roughly in line with the global figure of 40%. Hackers are the main perpetrators of external fraud in the region, instigating 41% of external economic crimes. Customers are the second most common perpetrators of external fraud, with a report rate of 35%.

You may think you know your customers well. But how well do you really know them? In our survey, 35% of external fraud committed against organisations was carried out by its own customers. Proper customer due diligence, continuous monitoring and robust KYC processes are important parts of an effective fraud prevention programme.

Decoding the fraud triangle

The diversity of fraud actors – and the fact that most are internal to organisations – underline the reality that it's people who commit fraud, not machines or technology. The most critical factor in a decision to commit fraud is ultimately human behaviour.

When a fraud takes place, it's the result of a complex mix of conditions and human motivations that can be summed up in the three principal drivers of internal fraud – the fraud triangle.

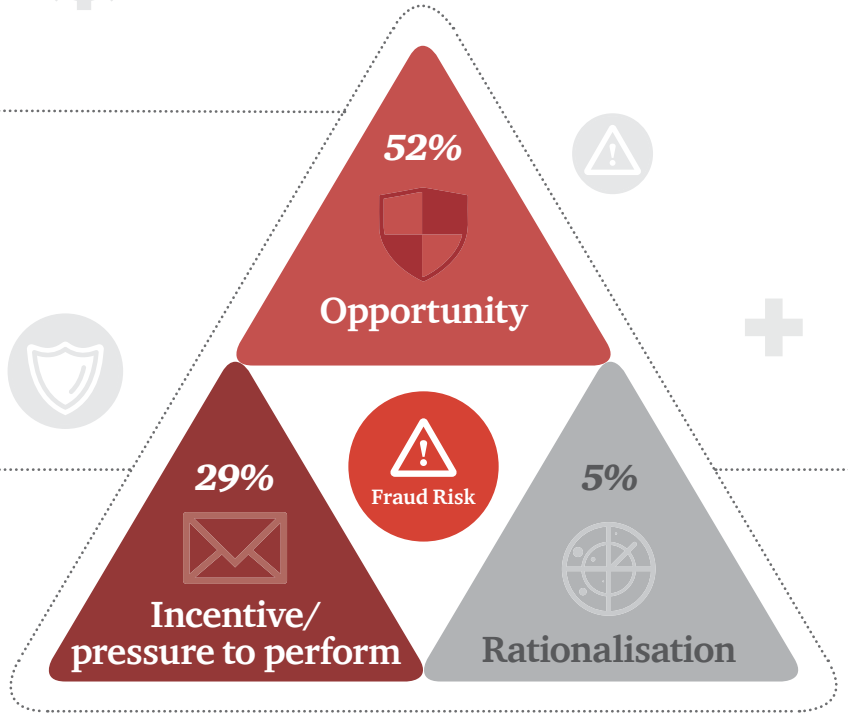
- Incentive / pressure
- Opportunity
- Rationalisation

While all three drivers must be present, their influence isn't equal. Historically, opportunity has been seen as the main contributing factor to fraud or economic crime – and that remains the case this year. This further confirms that investing in proactive measures and deterring fraud are key to closing the gaps of opportunity.

The problem and the solution

The antidote to opportunity: Controls.

Our survey shows that opportunity is regarded as the biggest contributory factor leading to fraudulent activity. One of the most effective actions that an organisation can take to curb rising opportunity is to implement clear and rigorous controls, through measures including policies, procedures, segregation of duties and codes of conduct.



Q. To what extent did each of the following factors contribute to the incident of fraud/or economic crime within your organization committed by internal actors?

Source: PwC's Global Economic Crime and Fraud Survey 2018: Middle East Spotlight

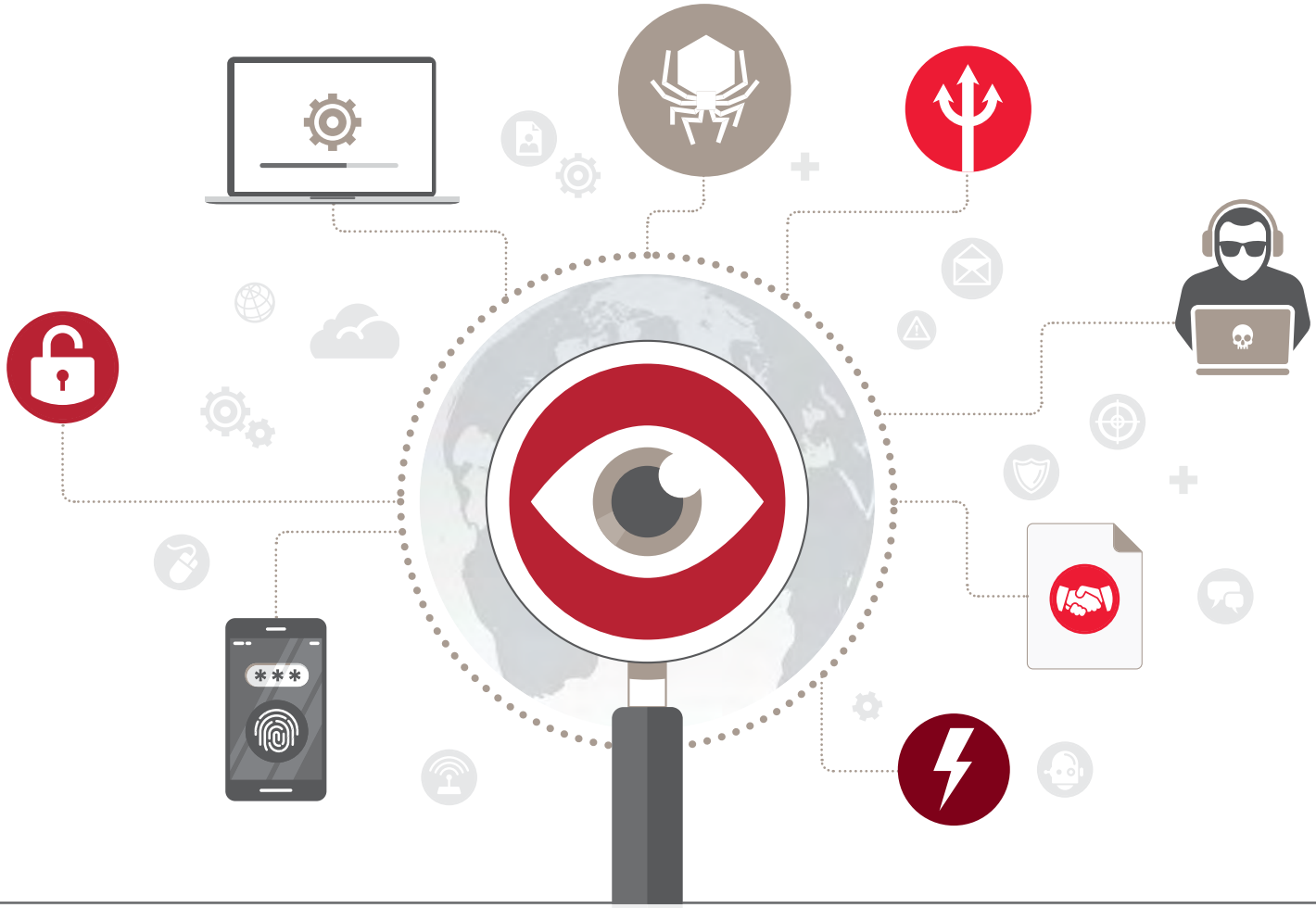
The antidote to pressure: Openness

The pressures and stresses that a workforce faces from both internal and external factors can lead to damaging effects in the long run. And steps to alleviate these pressures can dramatically reduce the likelihood of economic crime. These steps can include training, reporting, setting up whistle-blower lines and fostering a positive environment of coaching and development supported by an "open-door" policy. Ultimately, there's no better way to manage your people than to understand them.

The antidote to rationalisation: Culture

While opportunity and pressure can be measured and anticipated relatively easily, rationalisation is a much more difficult factor to tackle, since it is influenced by a vast range of factors and its characteristics vary from person to person. The first step is getting to know your people and what they expect of you as an employer, helping you to understand what makes them "tick" and build an inclusive culture. This culture should be reinforced through training and awareness programmes, and by maintaining organisational transparency and the right "tone from the top" in terms of both words and actions.

The dawn of proactivity



"If you think prevention is expensive, try having an incident."

Spending on anti-fraud activities is also set to rise faster in the region than elsewhere

Master your challenges and you will be better equipped to weather the storm

Against this background, what are organisations doing to stop the triangle tipping people into fraudulent activity? To do this, they need to close down the opportunities to commit economic crime by keeping up-to-date on threats and how to prevent, detect and respond to them. Our study shows that the proportion of organisations that have performed a fraud and economic crime risk assessment within the past 24 months has leapt to 77% from 47% in 2016.

…while also embedding an anti-fraud culture

Alongside specific measures to address fraud risks, it's also vital to develop an organisational culture that's founded on solid shared values, supported in turn by robust policies and an effective ethics and compliance programme embedded into everyday decision-making. Organisations in the region are certainly moving in this direction: as we highlighted earlier, the proportion of organisations in the Middle East with formal business ethics and compliance programmes has risen over the past 24 months. Spending on anti-fraud activities is also set to rise faster in the region than elsewhere.

Figure 7: In the last 24 months, respondents performed a risk assessment on one or more of the following areas

Be prepared – and emerge stronger: Key takeaways

Our 2018 Middle East Economic Crime and Fraud Survey confirms that many organisations across the Middle East are underprepared for fraud, for both internal and external reasons. It is imperative for an organisation to take proactive steps towards understanding fraud comprehensively by uncovering fraud blind spots and taking necessary action to prevent it. Here are the four key takeaways from our study, complete with actions related to each.

1. Know where you stand:

Enhancing your ability to identify and address your fraud risks can strategically assist you in preparing yourself to protect your organisation against these risks. Understanding your organisations' pressure points, both on a human and business front, can help to design your risk mitigation plans that will make the organisation stronger and more strategically agile in both good times and bad.

ACT NOW:

Key actions in the fight against economic crime can include performing periodic assessments of the risk of fraud and removing silos between functions like compliance, ethics, risk management and legal, and embedding a culture that is more cohesive, resilient and sensitive to fraud risks.

2. Tone at the top has a ripple effect:

Not only has the threat of economic crime intensified in recent years, but the rules and expectations of all stakeholders – from regulators and the public to social media and employees – have also changed irrevocably. In a world where reputations can be won and lost overnight, an organisation will be held accountable tomorrow for what happens today. So how leadership respond when a fraudulent event or compliance issue arises, will be as important to the organisation's future as the event itself.

ACT NOW:

Embedding transparency in your business and showing commitment to best integrity practices are more critical today than ever before and will strengthen the reputation of those organisations adopt it. Show your employees, business partners, customers, shareholder and the public your commitment to ethical standards.

3. Think outside the box:

The advancing role of technology in your organisation requires you to think of new ways to manage your risk of fraud and economic crime with greater focus on fraud committed by consumers and cybercrime being highlighted as some of the highest increasing threats.

ACT NOW:

Organisations need to consider new and more effective techniques in addressing the changing business environment influenced by the higher dependency on technology and need to think outside the box in addressing the evolving risks by utilizing the increasing amounts of data being captured by businesses.

4. Mature your three lines of defense:

Using your knowledge based on your organisations proactive measures combined with the lessons learnt from responding to fraud incidents to enhance the effectiveness of your three lines of defense – management, risk functions and internal audit – is fundamental to maturing your organisation's resilience.

ACT NOW:

Take the time to reflect on incidents taking place in your organisation to take active steps to enhance your defenses against economic crime. Developing the way you perceive and deal with evolving threats is integral in building strong principles of prevention and deterrence within your three lines defense.

Take these steps, and your organisation will be well-placed to transform a potentially serious business issue into an opportunity to stand out from the crowd. Put simply: be properly prepared for fraud – and rather than suffering a setback, you'll be able to emerge stronger.

Contacts

Nick Robinson
Partner, Forensic Services
+971 (0) 4 304 3974
+971 (0) 50 899 2087
Nick.e.robinson@pwc.com

John Wilkinson
Senior Partner, Forensic Services
+971 (0) 4 304 3538
+971 (0) 50 900 7491
john.d.wilkinson@pwc.com

Tareq Hadadd
Partner, Forensic Services
+966 (11) 211 0400 (ext 1880)
+966 (0) 56 091 1113
tareq.haddad@pwc.com

Achraf El Zaim
Partner, Forensic Services
+971 (0) 4 304 3132
+971 (0) 50 841 0383
achraf.elzaim@pwc.com

Mohammad Malkawi
Director, Forensic Services
+971 (0) 4 304 3344
+971 (0) 56 676 1980
mohammad.malkawi@pwc.com

Aaqilah Zahra Nagdee
Manager, Forensic Services
+966 (11) 211 0400 (ext 1190)
+966 (0) 56 619 2840
aaqilah.z.nagdee@pwc.com

Timur Korshlow
Director, Data Analytics
+962 (0) 6 500 3486 (ext 3332)
+962 (0) 7 9296 4770
tkorshlow@pwc.com

Sion Rhys
Director, E-discovery
+971 4 515 7479
+971 52 650 2199
sion.l.rhys@pwc.com

David Hall
Director, Global Intelligence
+971 4 5178810
+971 56 6762919
david.hall@pwc.co m

www.pwc.com/me/crimeandfraudsurvey

31219 Design Services (03/18)