# *Adjusting the Lens on Economic Crime in the Arab World*

**26%**

of organisations report being victimised by economic crime

**30%**

Cybercrime remains 2nd most reported economic crime affecting organisations

**63%**

indicated that opportunity or ability is the main factor for committing an economic crime

pwc

*www.pwc.com/me/crimesurvey*

# Leading observations

## 1 Economic crime an evolving obstinate threat

- Increase in organisations reporting economic crime in the Middle East (26%) compared to 2014 (21%)
- Internal audit was able to identify more incidents in 2016 (10%) compared to 2014 (5%) but still below the global average
- 17% of reported cases of economic crime were uncovered by accident, a rate much higher than the global average (11%)

***What opportunities are available for countering economic crime proactively?***

*Economic crime is a diversified global issue*

## 2 Controls must be embedded in organisational culture

- Opportunity or ability to commit the crime is cited as the most prevailing factor (63%)
- Gap between internal and external fraud actor is closing
- 1 in 4 respondents have never carried out a fraud risk assessment

***What are the risks your business faces and do you actively identify vulnerable areas?***

*Financial damage extending to the hundreds of millions of US dollars in some cases*

## 3 Cyber threats climb, but business preparation is not keeping pace

- Cybercrime remained the 2nd most reported economic crime affecting 30% of Middle East organisations
- Most companies are still not adequately prepared for or even understand the risks faced: Only 33% of Middle East organisations have a cyber-incident response plan
- Engagement of leadership is critical, but less than half of board members request information about their organisation's state of cyber-readiness

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

*Cyber preparedness can be viewed as an organisational stress test*

## 4 *Disconnect between tone at the top and reality on the ground*

- More than 1 in 5 Middle East respondents not aware of the existence of a formal ethics and compliance programme and many are confused about ownership for the ethics & compliance programme
- A third of the incidents of serious economic crimes were perpetrated by internal parties
- Employee morale (42%), business relations (35%), reputational harm (34%) and regulations with regulators (29%) cited as top forms of damage

***Are your organisational values well communicated and understood by everyone in your organisation? Are the leaders setting examples in adhering to these values?***

*People and culture are your first line of defence*

## 5 *Anti-Money Laundering continues to confound*

- 1 in 6 financial institutions in the Middle East have experienced enforcement actions by a regulator: Failure to curb illicit business practices may lead to personal liability
- More than one fifth of Middle East financial services firms have not conducted AML/CFT risk assessments across their global footprint
- Cumbersome legacy systems plague compliance efforts
- Data quality cited by 35% of respondents as a significant technical challenge
- Lack of experienced AML/CFT staff a major issue

***How would your organisation fare in the face of regulatory scrutiny?***

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

# Contents

# Foreword

We are pleased to present to you our third edition of the Global Economic Crime Survey – Middle East report 2016.

Economic crime continues to forge new paths into businesses with increasingly complicated threats that are challenging the balance between resources and growth. Regulatory compliance is also becoming more complex adding layers of stress and burden to responsible businesses.

This year, three specific areas have contributed to the trends of economic crime over the last two years:

1. The importance of ethics and organisation culture has proven to be key in the fight against economic crime. Controls alone are not enough if organisations do not have strong cultures and values that promote the right behaviour;

2. The ever increasingly complex crime involving cyber promises to threaten organisational growth and reputation; and

3. Money laundering has become an important aspect of compliance, not just for the financial services, but for all sectors.

Our report challenges you to adjust your lens on economic crime and refocus your strategic path to prepare your organisation. We also hope you find this report a useful tool to consider the risks your organisations face and enhance your control mechanisms to prevent, detect and respond to economic crime.

Incorporating the views of respondents from 12 Arab Countries, makes this report one of the most comprehensive studies in the Middle East. Our thanks to all the respondents and organisations that made this Middle East report possible.

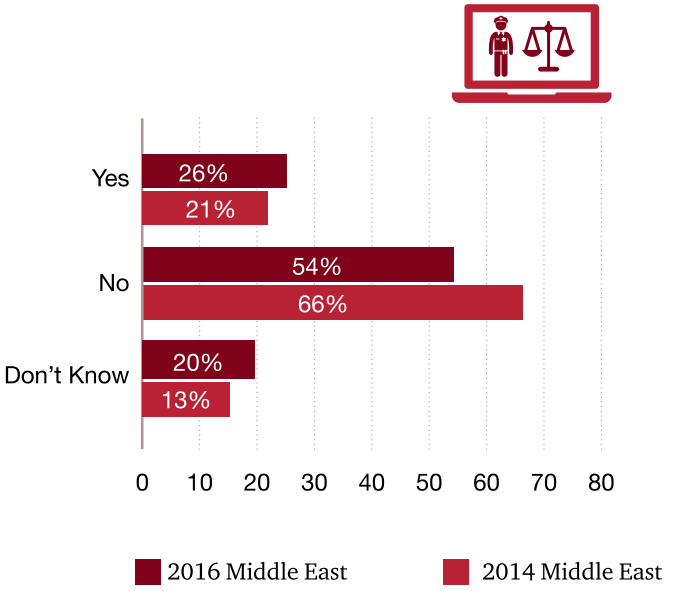
***Nick Robinson***
Middle East Forensic Services Leader

***Tareq Haddad***
Middle East Investigations Leader

# Overview

PwC has been surveying trends in global economic crime since 2001. In that time, despite efforts to combat economic crime, there has been no clear indication that levels in the Middle East or globally have decreased. Economic crime remains as tough to tackle as it's ever been.

**Has your organisation experienced any economic crime within the last 24 months?**

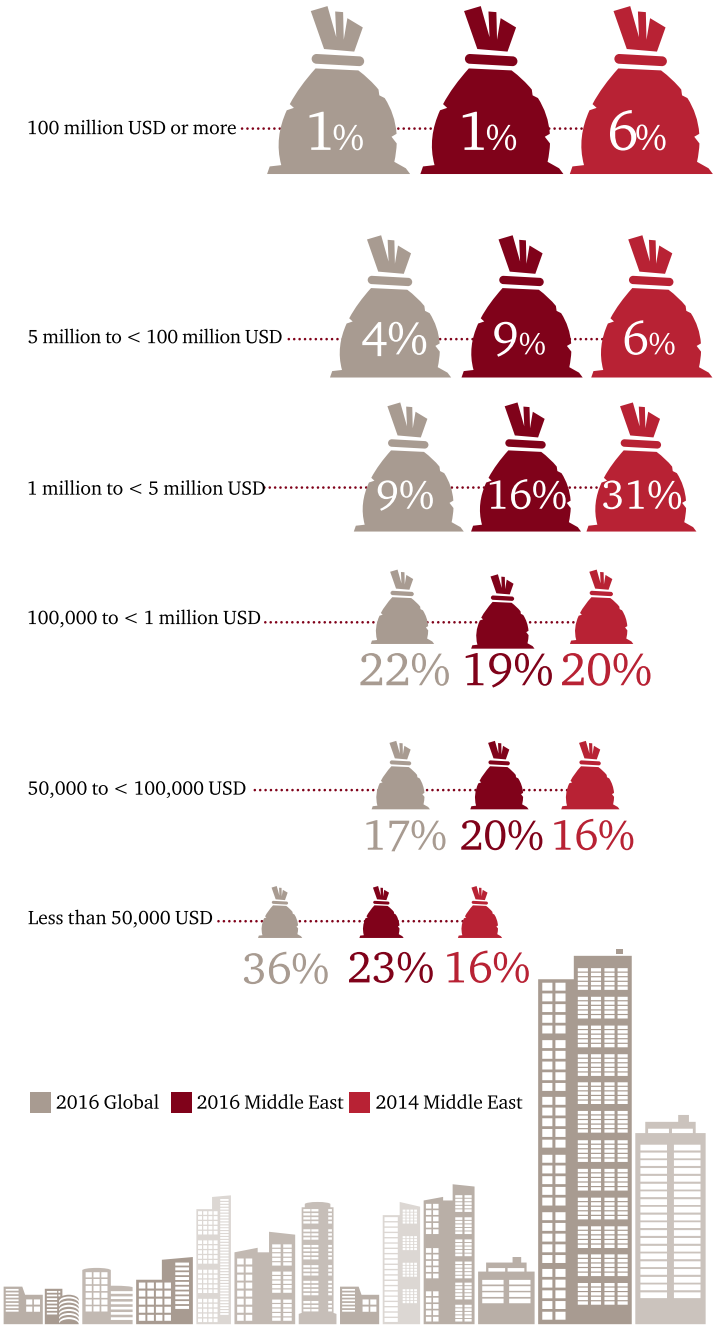



In the Middle East, 26% of respondents indicated that their organisation reported economic crime in the last 24 months. This is lower than the global average of 36%. While the reported number of affected organisations in the Middle East was lower, the number in the region who simply didn't know if they'd been a victim was much higher than the global average (20% against 11%). This is a cause for alarm, and points to a serious lack of trust by executives in their systems to identify economic crime as it occurs. A concern made all the more prominent by the fact that over 50% of the organisations surveyed had not, or did not know if they had conducted a fraud risk assessment during the previous two years.

When looking at the financial impact, the losses in the $5m to $100m range have gone up since the last survey, which is clearly a cause for concern. Also, more generally the increase in crimes for the category of less than $50,000 (despite the fact that it is still less than the global average) could indicate more pervasiveness of crimes within organisations in the Middle East compared to 2014.

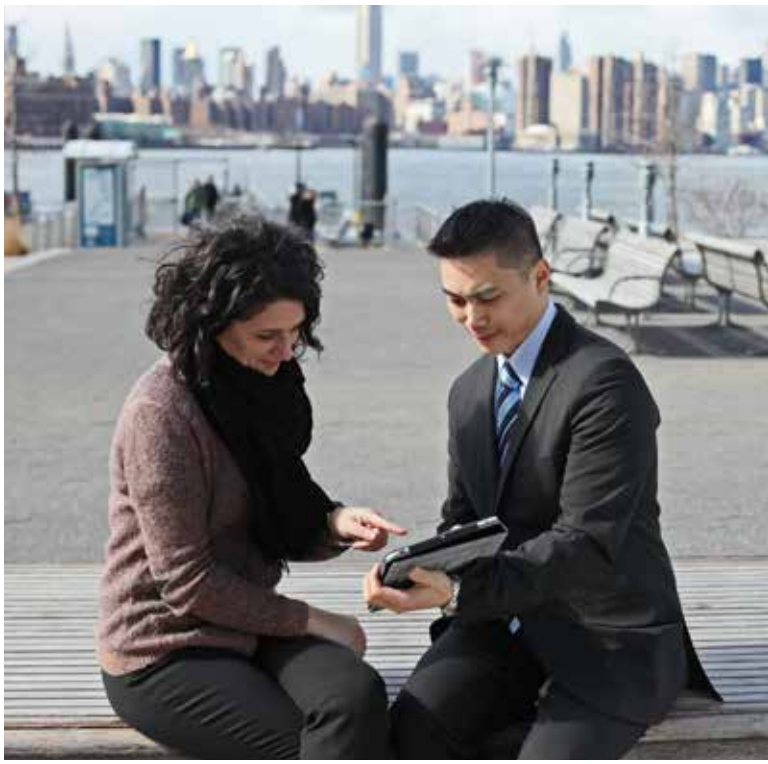
***Economic crime remains as tough to tackle as it's ever been***

**Approximately how much do you think your organisation may have lost through economic crimes over the last 24 months?**

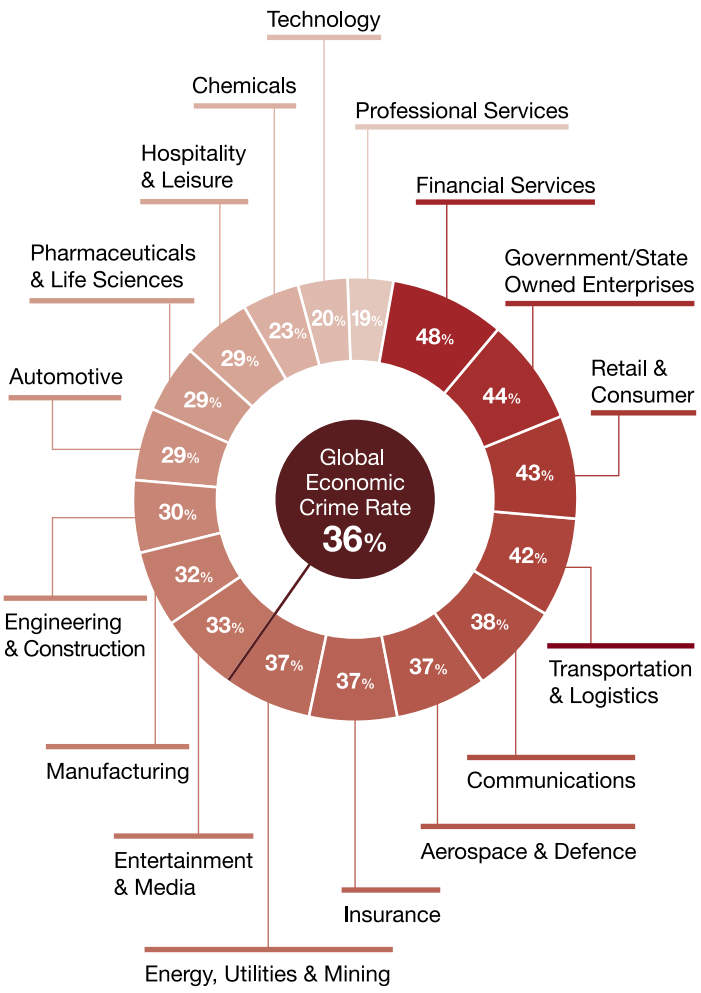



## *How does the Middle East compare to the rest of the world*

| 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 | 26% | 21% |
| **Global** | **36%** | **37%** |

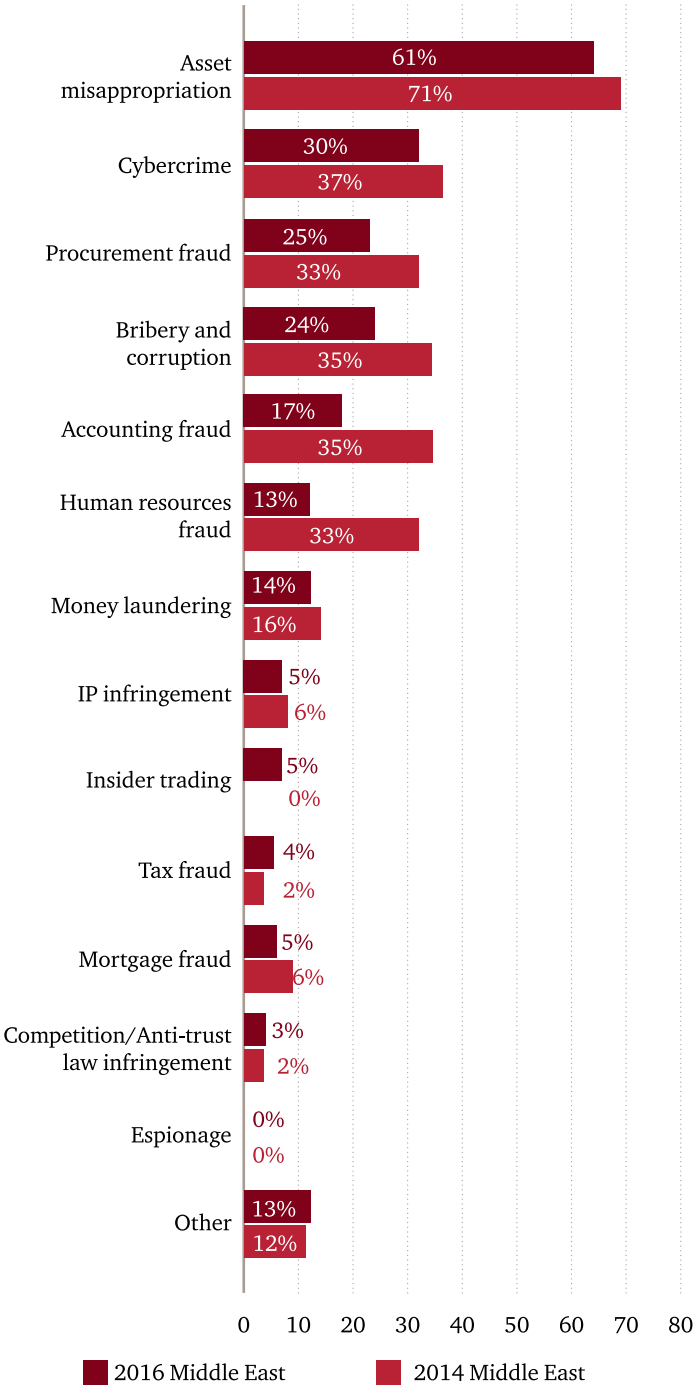


## Global view: Which industries are at risk?

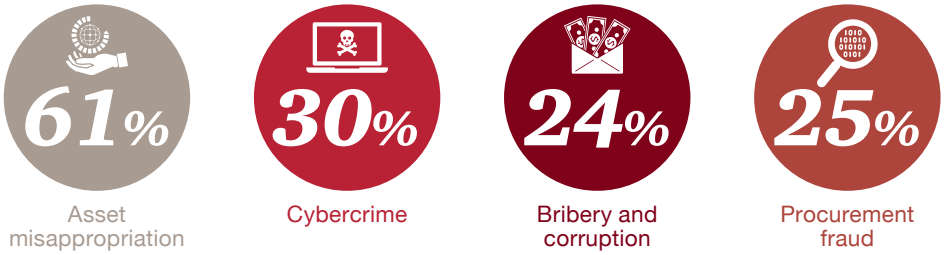



On a global basis, and in the Middle East, reported incidences of asset misappropriation, bribery and corruption, procurement fraud and accounting fraud all showed declines. The declines were more marked in the Middle East as shown below. However globally, cybercrime jumped to 32% (up 8% from 2014) whilst the Middle East showed a decline in cybercrime of 7%.

## Types of economic crime experienced



**Top 4 most commonly reported types of economic crime in 2016**




So at face value, things are getting better. But does that paint a true picture? With overall incidences of economic crime rising in the Middle East, and an identified failing of organisations to focus efforts on identifying fraud risks, it would be unwise to jump to such conclusions.

Organisations in the region should not be lulled into a false sense of security if the level of reported incidents in their organisations seem lower than in the past, but should consider the effectiveness of their fraud detection mechanisms.

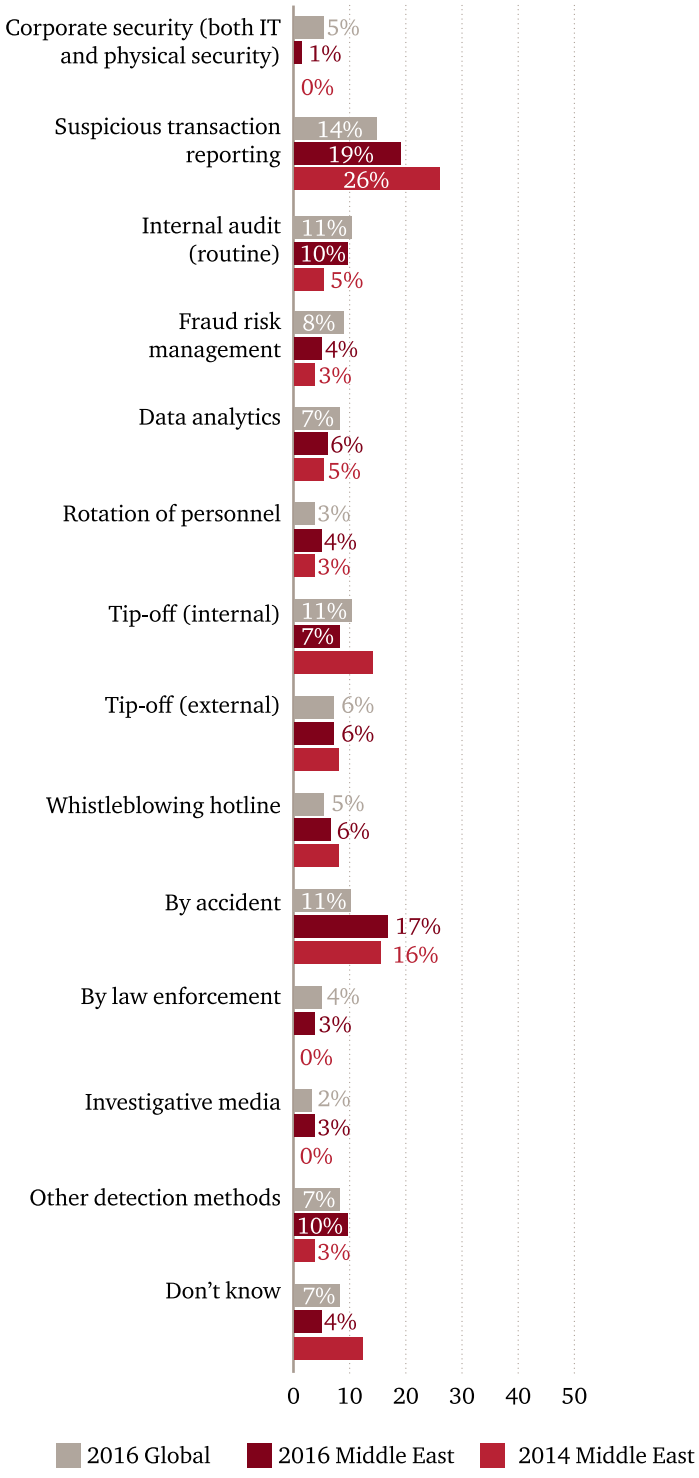
If the fraud detection methods are limited by being too reactive, too irregular, and aren't keeping pace with either the change, or the growing sophistication in complex areas like cybercrime, then the number of identified instances will naturally decrease. A telling finding here is that respondents in the Middle East indicated that accidents uncovered 17% of reported economic crime, a rate which is much higher than the global average of 11%, and has increased compared to our previous survey.

On a more positive note, the role of internal audit in detecting fraud is reported to have become more effective compared to 2014 despite it being slightly below the global average. However, what is also apparent from the results is that economic crime reported through tip-off and whistleblowing has decreased in the Middle East in 2016 compared to 2014.

This should again trigger some alarm bells in the C-suite. Use of such reporting mechanisms can be indicative of the culture and tone of ethics and compliance within an organisation, and here there is clearly still significant work to be done.

***Spotting economic crime by accident remains one of the most common ways of detecting incidents***

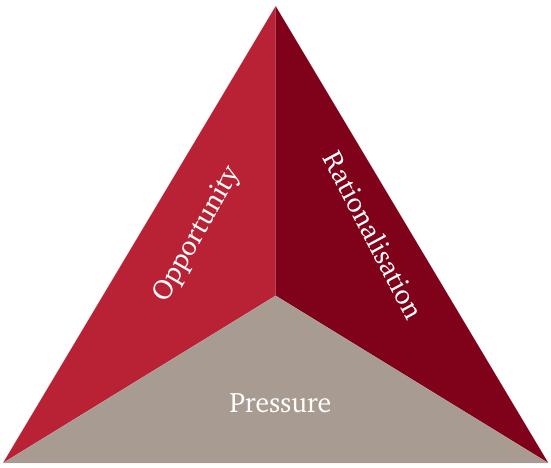
**How did your organisation initially detect the most serious economic crime it experienced within the last 24 months?**



## *The causes of economic crime*

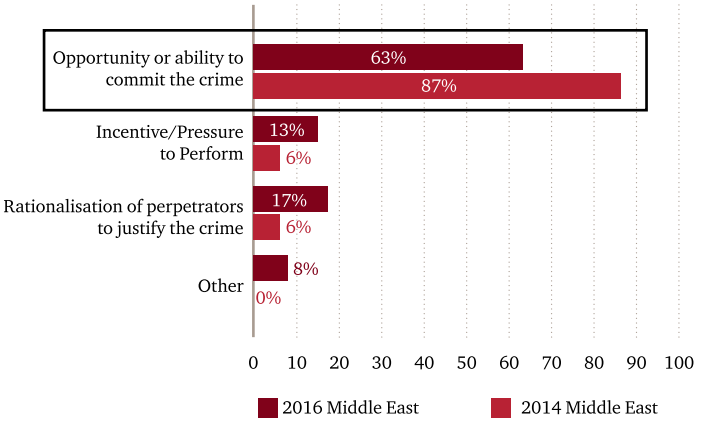
So what's driving the rise of economic crime? One factor is that crime will always occur where there's the opportunity to commit it, and that opportunity continues to exist. In combating fraud one has to consider the 'fraud triangle', and all three elements of that need to be in place for a crime to take place.

### The Fraud Triangle




But in our experience this is not an equilateral triangle – opportunity is a far more significant component than the other two. 69% of the global respondents to this year's survey, and 63% of those in the Middle East, cited opportunity as the biggest factor driving crimes committed by employees.

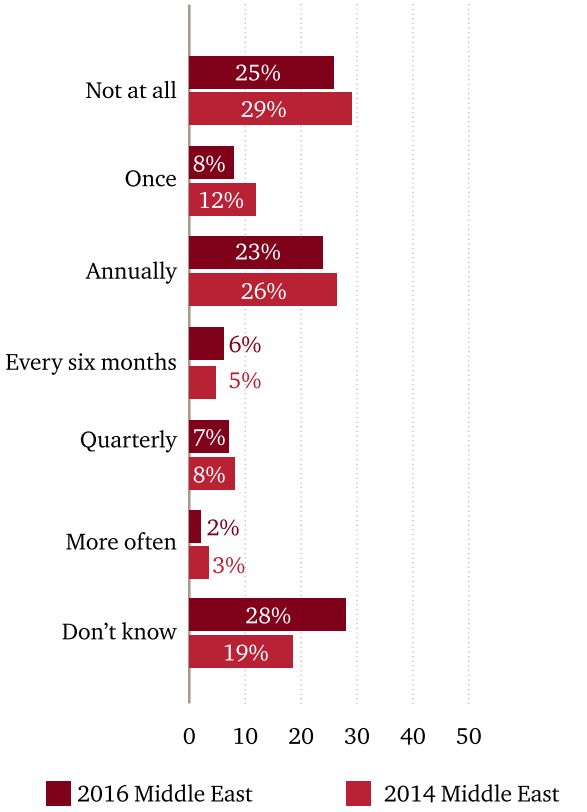
**What contributed the most to economic crime committed by internal actors?**




Therefore, addressing the opportunity factor in organisations has a greater effect on reducing the level of economic crimes. And there is clearly room for improvement here with 25% of respondents in the Middle East indicating that their organisations have never performed a fraud risk assessment.

Reducing the rationalisation and pressures on individuals to commit economic crime can also play a significant role. That's why culture and the ethical standards of the organisation are so vital. We explore this further in our deeper dive into Ethics & Compliance in the following sections.

**In the last 24 months, how often has your organisation performed a fraud risk assessment?**




The challenge for businesses then, is to close down the opportunities to commit economic crime. Part of this is about keeping up-to-date on new threats and new ways to prevent, detect and respond effectively to those threats. But it's also vital to ensure that the organisation has a culture based on strong shared values, which is supported by robust policies, and a rigorous ethics and compliance programme which is integrated into day-to-day decision-making.

***Economic crime is a risk that is hard to unseat. Constantly evolving and seeking new forms, it requires constant vigilance from the Boardroom via the C-suite to middle management and the shop floor. But some Middle Eastern organisations have perhaps adopted a one-time; one solution approach to this challenge which is reactive, irregular and inconsistent. Unfortunately this is like cutting the head off a hydra. Others quickly grow back. The battle to combat economic crime is not so easily won.***

# *Ethics & 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 realising your opportunity.

# Aligning decision-making with values

Companies around the world have found that strong ethics programmes are key to counter economic crime in all its forms. The many corporate scandals that have emerged over the last year have proved – if we didn't know it already - that economic crime is a question of corporate culture and values, not just a question of compliance. Even the best and most rigorous compliance programme will fail if a company's culture allows, ignores or accepts wrong-doing.

The Middle East faces some particular challenges here, because organisational cultures are challenged by a diverse and often dynamic environment. Many Middle Eastern companies have grown fast, and their processes and procedures have not kept pace – whether in this area or more generally. Furthermore, Middle East organisations suffer often from much less clarity about roles and responsibilities. This lack of awareness might cause personnel to overlook some important aspects of their functions within their organisations. A lack of clarity also makes it more difficult to drive accountability when events take place.

Organisations in the region can also tend to rely heavily on buying in IT or controls systems, with the assumption that this has 'fixed the problem'. But technology alone is never enough, and needs to be supported by competent and trained teams to operate it and by a corporate culture that does not tolerate wrongdoing. Companies need skilled people for specific compliance roles, but ethics can and must be everyone's responsibility.

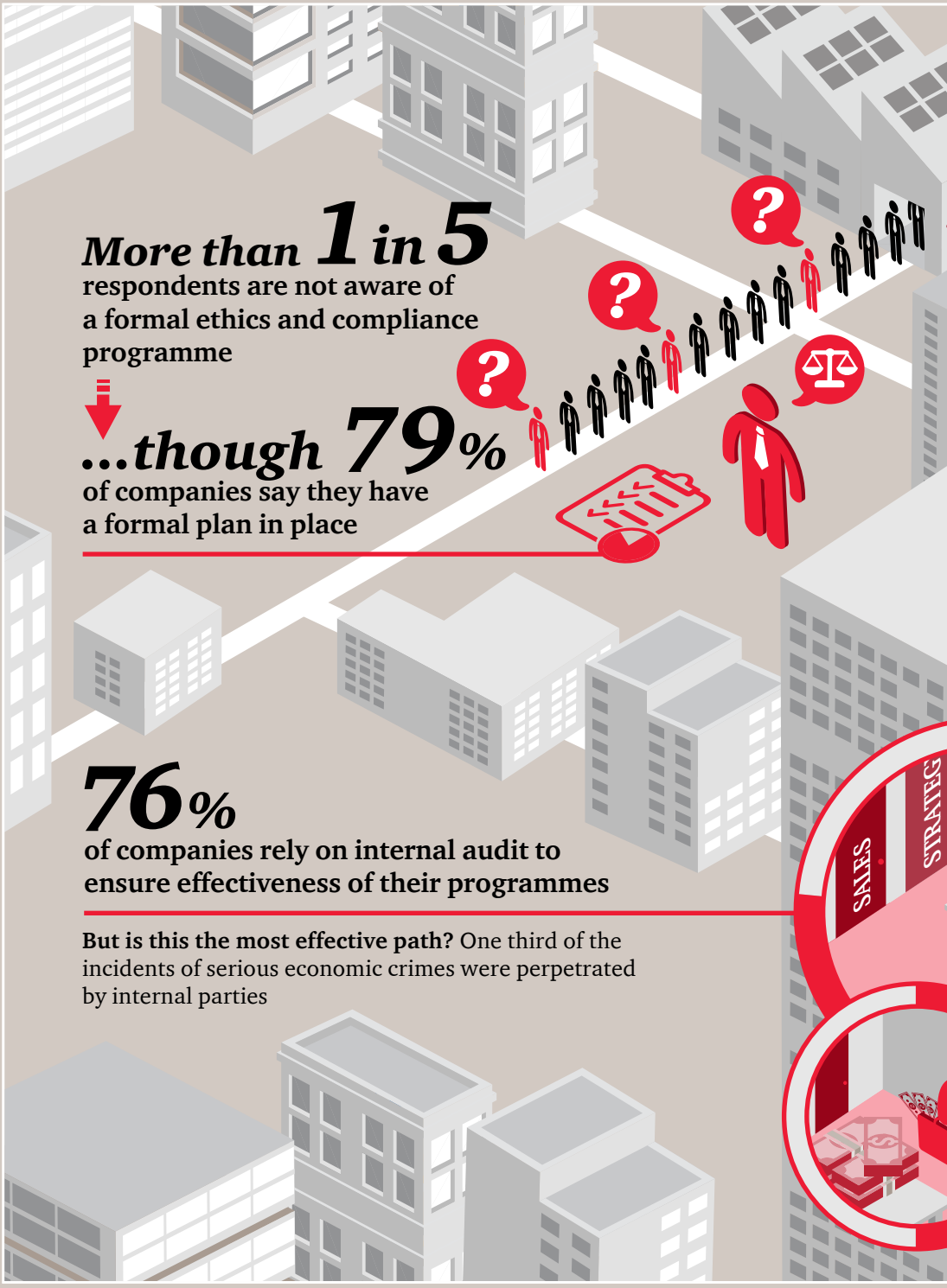
## People and culture

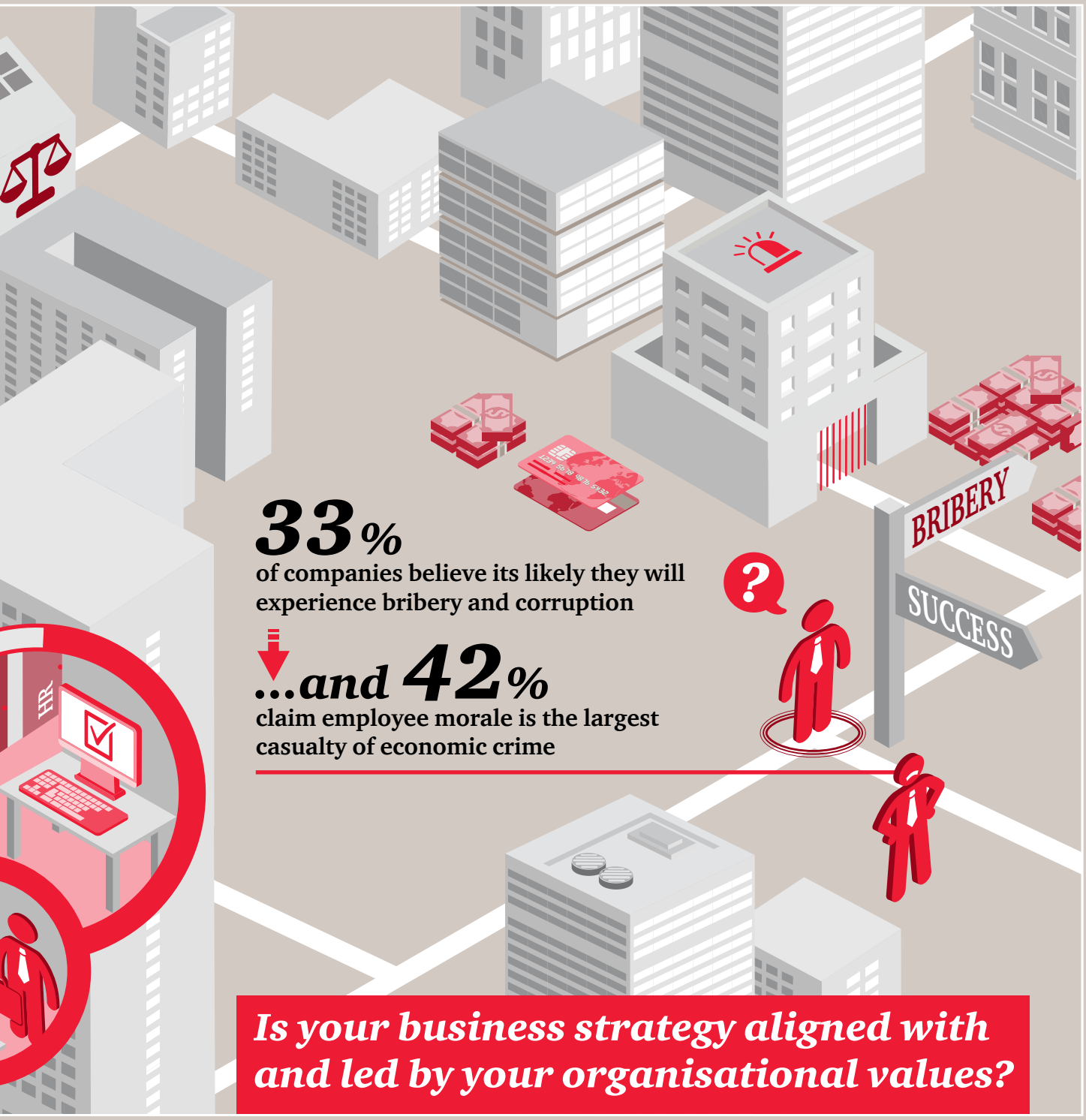
The high-profile global corporate scandals of the last few years have affected companies in a wide range of sectors and many different markets, but one thing has tended to characterise them all: they were failures of culture, not of compliance. Some of these businesses were extremely heavily regulated, with detailed 'best practice' ethics programmes, and yet none of those measures prevented the wrongdoing. That's because the values that really applied in these businesses were at odds with those at the front line. The failures happened because the organisations' leadership believed the latter, and were blind to the former.

When asked about their organisations culture, 85% of Middle Eastern respondents state that they have a comprehensive Code of Conduct, supported by regular training (60%). They also told us their Board believes the organisation's values are well understood (84%), that ethical behaviour is part of their HR procedures (77%), and their senior leaders convey the importance of ethical business conduct in all that they do (74%).

This all looks fine on paper, though are the messages from the top actually conveying the culture senior management believe? The answer has to be no.

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

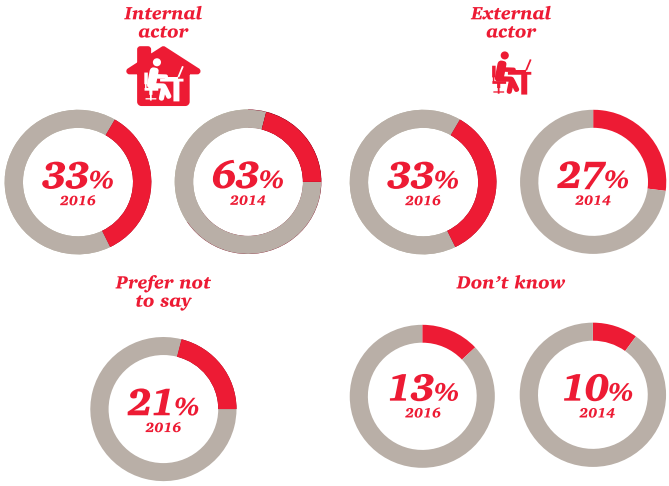



33%
of companies believe its likely they will experience bribery and corruption
...and 42%
claim employee morale is the largest casualty of economic crime
BRIBERY
SUCCESS
HR
Is your business strategy aligned with and led by your organisational values?

## To what extent do you agree or disagree with the following statements about your organisation regarding its business ethics and compliance?

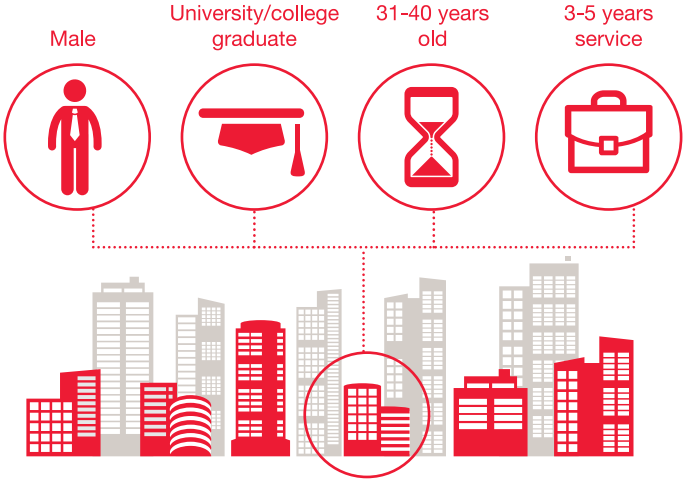

33% of all the economic crimes reported in the last two years were committed by staff. And many more could have been involved in some degree of collusion, either between outsiders and insiders, or within the organisation.

## Who was the main perpetrator of the most serious economic crime your organisation experienced in the last 24 months?



Looking at the bigger picture, what the results are telling us is that there is often a dangerous disconnect between what CEOs and Boards believe is happening, and what is actually going on. And this is a problem across the globe. However, the degree of distance in the Middle East between the most senior managers and all other staff tends to be much wider, which will exacerbate this corporate disconnect. In purely practical terms, it also reduces the amount of scrutiny on the next level down. This may explain why the most likely fraudster in the Middle East is in middle management (29%) or a junior role (46%), with three to five years' service - this goes against the trend towards more involvement by senior employees that is evident from the global results this year. This may also explain why some types of fraud are more prevalent in the Middle East: 50% said their HR-related frauds included the misclassification of payroll expenses (17% globally), 50% had received false wage claims (40% globally), and 20% reported fraudulent reductions in payroll taxes (7% globally).

**Most likely characteristics of internal fraudster**




Boards and top teams need to understand what's really driving behaviour in their organisations, and build a positive culture that incentivises the behaviour they want. One way to do this is to link compliance more firmly to values, rather than a separate box-ticking activity. In regions like North America and Europe, companies are devoting significant resources to values programmes, which tend to be more firmly embedded in their HR strategy and internal communications campaigns. It's a measure of the relative developing corporate culture in the Middle East that this sort of activity is often under valued here. The priority, therefore, is to ensure that organisations are adequately protected against economic crime, as their corporate cultures evolve.

So, a further wake-up call to Boards and Management of organisations. The efforts believed to be expended on culture are clearly not having the desired effect. It's time to look in the mirror and ask, 'have I really done all I can do to reduce my employee's rationalisation of inappropriate acts?'

## *Bribery and corruption*

Bribery and corruption remains a problem across the world, but it's a particular and persistent issue in the Middle East. The good news is that a number of the major economies in the region have made progress in this area, with the ratings for Kuwait, Jordan, and Saudi Arabia all improving slightly in the Transparency International Corruption Perception Index for 2016.[1] This is the third consecutive year that Saudi Arabia has improved its standing. That said, there has been little progress elsewhere in the region: Egypt, Libya, Morocco, Syria, and Tunisia have deteriorated slightly, and three of the bottom ten countries are from the region, namely Iraq, Libya, and Sudan, all of them countries affected by conflict.

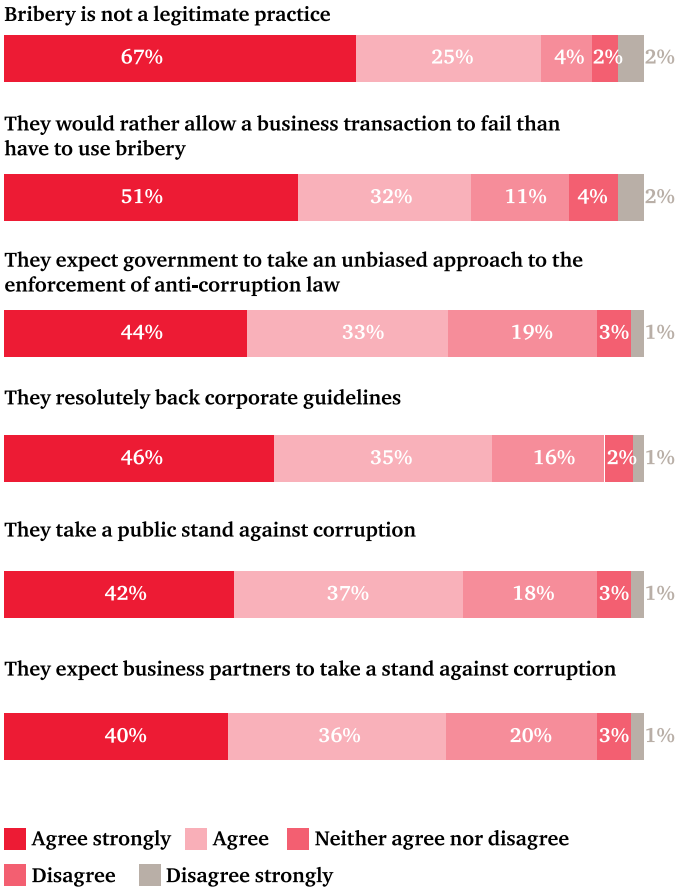
24% of the Middle East respondents who'd experienced some form of economic crime in the last two years had also been the victim of bribery or corruption. That's in line with the global average, and down from 35% in 2014, but it's important to note that 33% expect to experience it again in the coming two years, compared with 24% globally. 38% also expect to suffer procurement fraud in the same period, compared with 26% globally.

Organisations in the region need to remain vigilant about this sort of crime, and do more to prevent it, especially due to the priority being given to this issue by international and national regulators in the US and EU.

***33% expect to experience bribery or corruption in the coming two years, compared with 24% globally***

Our survey respondents in the Middle East were all resolutely opposed to corruption, saying that bribery is not seen as a legitimate practice in their organisation (92%), they would rather lose a sale than pay a bribe (83%), and they're prepared to take a public stand against corruption (79%). Only 6% say they've been asked to pay a bribe in the last two years and only 9% say they lost business to a competitor as a result.

**How do you think your colleagues perceive the way your top level management deals with corruption?**



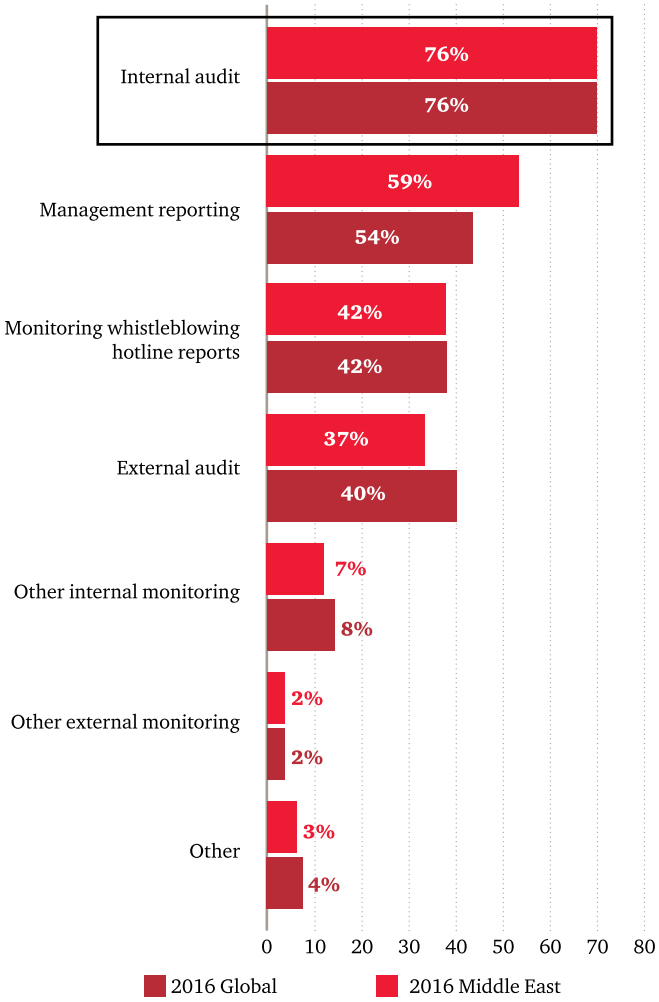

1) http://blog.transparency.org/2016/01/27/middle-east-and-north-africa-why-corruption-is-fuelling regional-insecurity/

## Compliance and programmes

As the survey results demonstrate, the risks companies face are not just increasing but are also becoming more complicated. As the authorities struggle to keep pace, regulatory oversight is growing too. It all adds up to an increasingly complex and expensive compliance burden, and many companies in the Middle East do not have the resources needed to deal with this properly, whether in terms of skills or the sheer numbers of people required.

According to this year's survey, 79% of Middle Eastern respondents have some sort of formal ethics and compliance programme, but only 60% support it with regular communications and training, which opens up the risk of an effectiveness gap. Likewise 76% rely on Internal Audit to assess their programme's effectiveness.

**How does your organisation ensure that your compliance and business ethics programme is effective?**




Given that Internal Audit, certainly in the Middle East region, is prone to be reactive and with limited resources, there's a very real risk that this approach will fail to spot new or emerging threats. As in so many other aspects of economic crime, a false sense of security can easily be the unintended consequence. And even though 42% of respondents in the region have seen an increase in their compliance spend in the last 24 months, and 48% expect an increase in the next two years, many of these organisations are in the heavily regulated financial services sector, and companies outside that sector tend to have more limited resources. Either way, investment in compliance has to be spent wisely, and on the right things. This includes new skills and capabilities, and technological tools that can handle vast amount of data, and identify trends proactively. But as we've already observed, technology is only part of the answer, especially without proper implementation and ongoing training. It's a combination of people and technology that make the best defence.

A good compliance programme will combine management reporting with real-time monitoring so that incidents can be spotted quickly if they do occur, and prevented wherever possible. It should focus on people and culture, reflect the company's specific risk and geographic profile, and be clearly aligned with corporate strategy and operations. For example, unexpected spikes in activity in specific markets or business units are often an early warning that someone's found a way to perpetrate crime. The right type of data systems can help you detect this.

And finally, a good compliance programme should be embedded in the organisation's HR processes, especially the disciplinary and reward mechanisms so that 'doing the right thing' is reinforced by both incentives and sanctions.

In other words, compliance should be the highly visible 'glue' that binds together values, policies, and decision-making, supported by comprehensive communications and tailored risk-based training. If done well, this approach can reduce the costs of economic crime, protect the brand and reputation, enhance employee morale and attract the best talent.

# 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 boundless threat

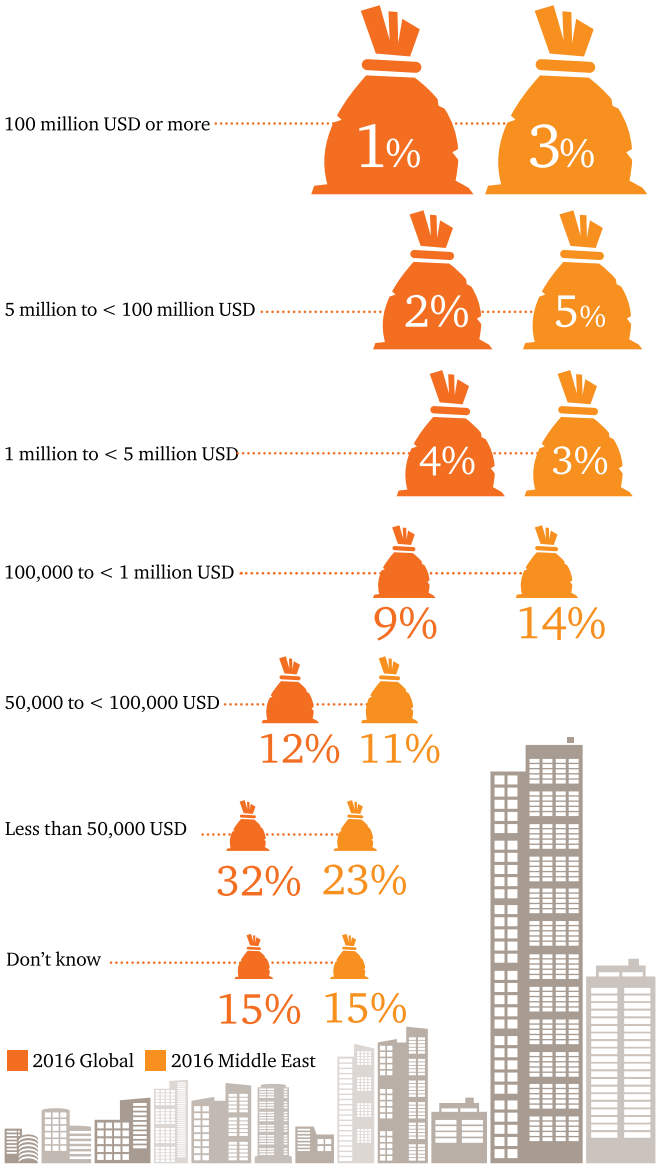
Cybercrime is one of the headlines of this year's global survey, which is no surprise, given it has been hitting the news more frequently over the past two years. It's jumped in terms of reported incidents and is the only type of economic crime to show a significant increase since 2014.

30% of Middle Eastern respondents who've suffered economic crime in the last two years have also been the victim of some sort of cyber incident. That's down from 37% in 2014, but any sense that this is a declining problem is contradicted by the number of high-profile cyber-attacks involving Middle Eastern companies in the last few months.

21% of respondents in the region didn't know if they'd been a victim of cybercrime, and many of those who answered no were probably victims as well, they're just not aware of it. Just over a quarter of those who admitted they'd suffered cybercrime told us there had been no financial loss as a result. Given that many Middle Eastern organisations see their brand or reputation as their single most important asset, it's significant that 42% of respondents in the region said they'd suffered high or medium-level damage to their reputation as a result of cyber-attacks, compared to 30% globally.

***21% of respondents in the region didn't know if they'd been a victim of cybercrime***

**How much do you think your organisation may have lost through cybercrime incidents in the last 24 months?**

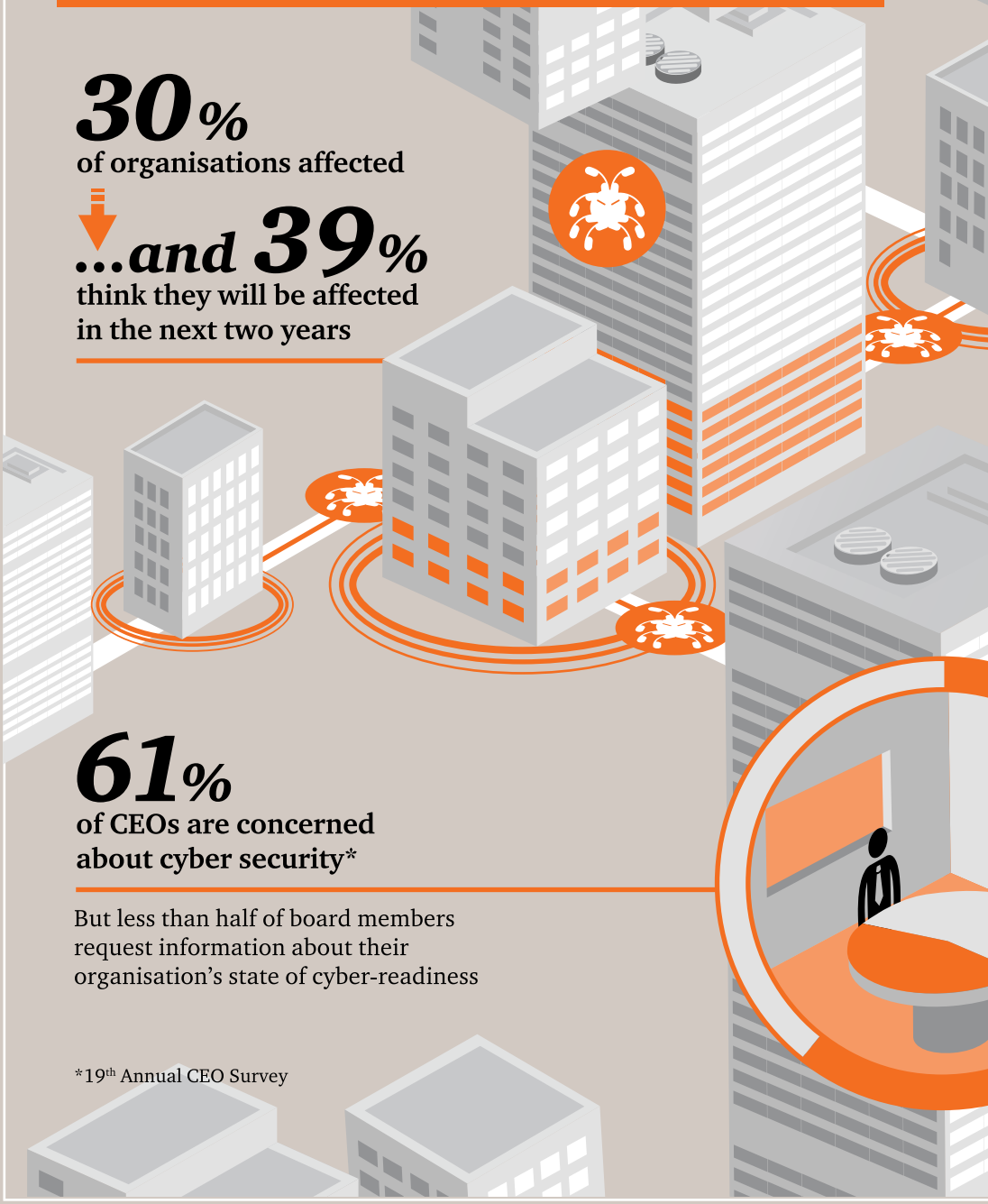


Cybercrime continues to escalate in a hyperconnected business ecosystem – jumping to 2nd most reported economic crime

## *Cybercrime remains to the second most reported economic crime...*

**30%**
**of organisations affected**

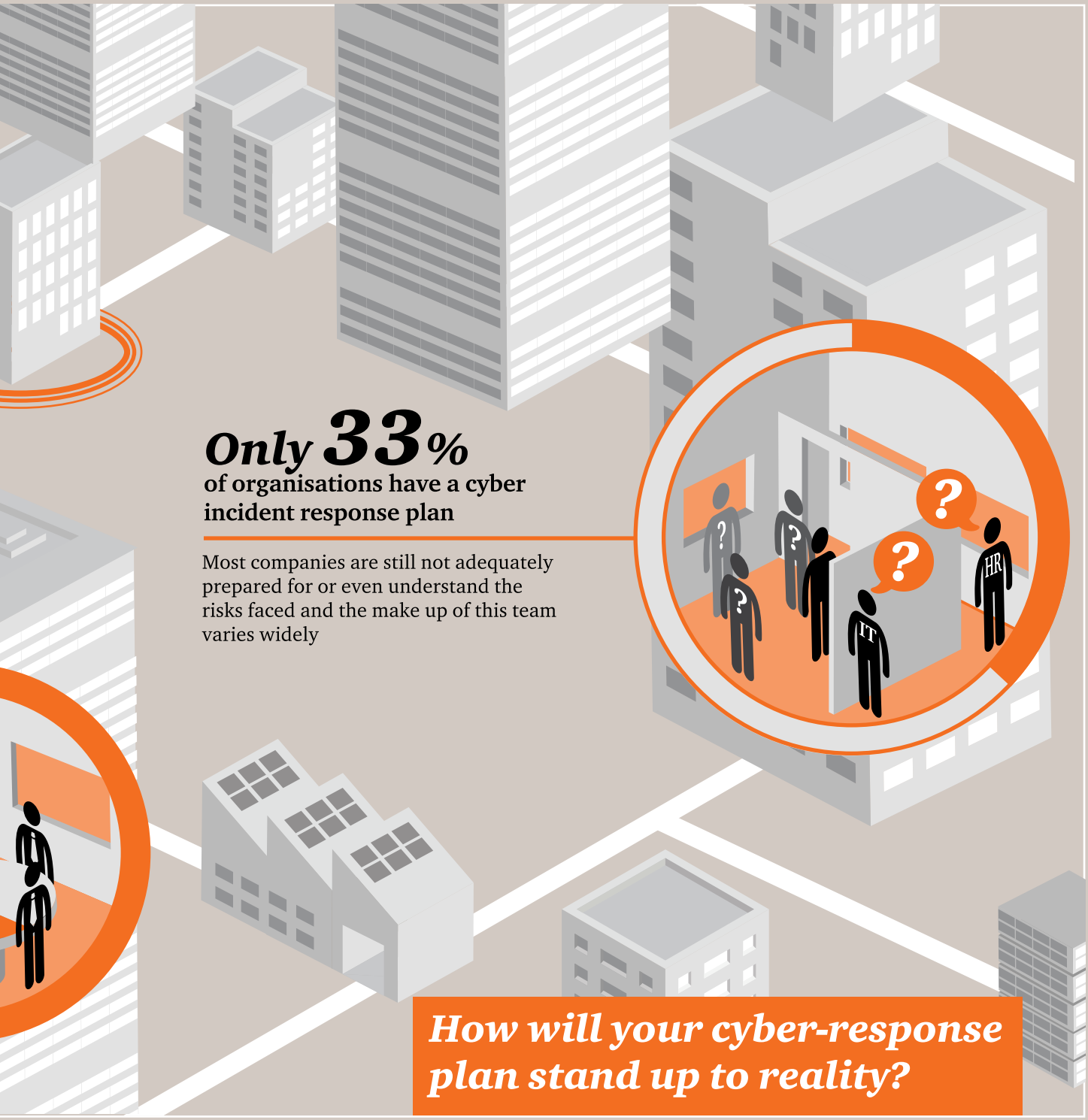
***...and 39%***
**think they will be affected in the next two years**



**61%**
**of CEOs are concerned about cyber security***

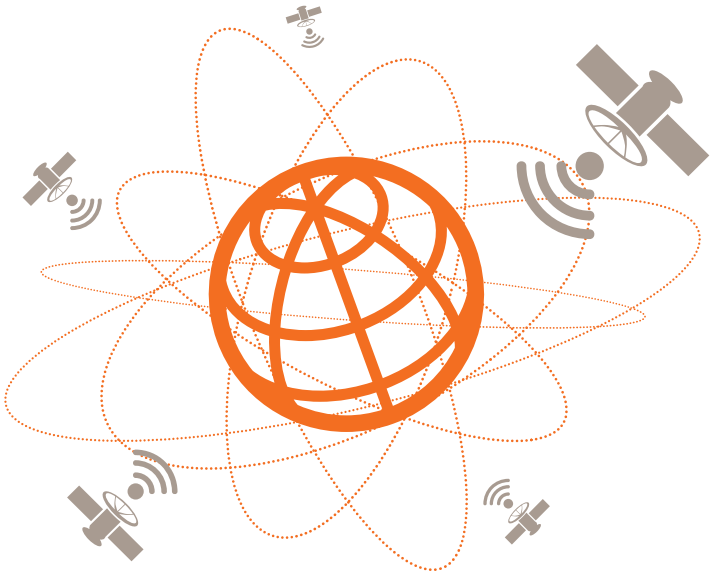
But less than half of board members request information about their organisation's state of cyber-readiness

*19th Annual CEO Survey


Only 33%
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
HR
IT
How will your cyber-response plan stand up to reality?

Cybercrime is affecting everyone, across all countries and all sectors, even those that might have thought themselves immune. According to PwC's Global State of Information Security Survey 2016 (GSISS), it was the retail sector that saw the most significant increase in cybercrime in 2015. Financial services has levelled out, even though it remains a prime target, not least because of the volume of personal information retained by the financial services sector. The GSISS also demonstrates that the threat of cybercrime is as much internal as it is external - 30% of all incidents were perpetrated in 2015 by current employees, and there is evidence that this is rising at an alarming rate.

So cybercrime is costing organisations dearly, not just in financial terms, but in the damage done to brands, reputations, share prices, trading relationships, and employee morale. One reason for the steep increase this year is the rise of cloud-based storage and the growing prevalence of the 'internet of things', with machines like smart televisions, smart watches, and home surveillance systems all connected to a network and therefore vulnerable to hackers. And those hackers are more ambitious than ever before, targeting not just credit card or financial information but the sort of 'crown jewels' that can bring down an entire business if they're stolen, whether that's Intellectual Property, commercially sensitive information, or operational data that can be encrypted by malware and held to 'ransom' until the victim pays to get it back.



## **Threat:** 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

The most significant conclusion to be drawn from all this is that cybercrime is no longer an IT problem. It's a business risk like any other, and one that promises to limit the growth and development of organisations if it is not managed properly. That means having the right people, the right processes, and the right governance, fortified with the right technology. It means making cyber issues an integral part of routine risk assessments, with active oversight from the Board. In PwC's 19th Annual Global CEO Survey, 61% of the respondents said they were concerned about cyber risks, but at the moment only 39% of the Middle Eastern Boards in our survey ask for any information about their organisation's readiness to cope with a cyber-attack. And a further 12% haven't even considered whether they need to have this data. But they clearly do. Involvement from the highest levels of the organisation is key to ensure that efforts are dedicated to fight this ever increasingly complex crime.

Boards need to map their digital footprint, so they can properly understand and assess the risks. To take just one example, there's been a spate of scams involving fake emails that appear to come from a company's CEO, asking for a money transfer to be made. The criminals usually time these for when the CEO is on holiday, to increase their chances of success, and many of them get the information they need to do that by tracking the social media accounts of the CEO's family members.

How many organisations thought of that scenario and acted to address the openness of critical information of social media often posted by their own CEO?

### *Crisis management: What to do if you detect a breach*

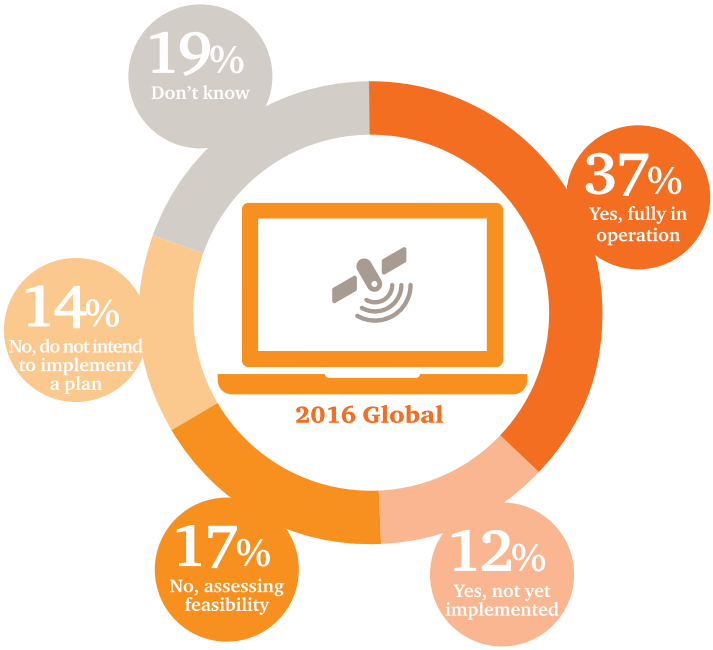
- Activate your crisis plan, and mobilise your first responder team.
- Get as much information as you can about the breach, and whether it's still ongoing. With the increasing complexity of data networks, it can be difficult to identify how the breach could have happened.
- Ensure that evidence is preserved and analysed by qualified and experienced responders as there are sophisticated forensic and data analytical techniques that organisations can use to respond in an efficient manner.
- Don't forget that some breaches are done as decoys, with the real target elsewhere in the network. These deeper incursions can be much harder to find, and it can take much longer.
- Decide whether to involve law enforcement, and what the appropriate agency would be. There are many factors to consider here, and they will vary according to the type and scale of the attack.
- Consider secondary risks. For example, if you use VOIP/networked phone services, your telephones are also likely to be compromised.
- Don't forget that the principles of any criminal investigation still apply. Your priority will be to stop the attack and get back to normal operations, but don't inadvertently destroy evidence that could help track down the perpetrators and prevent the next attack.

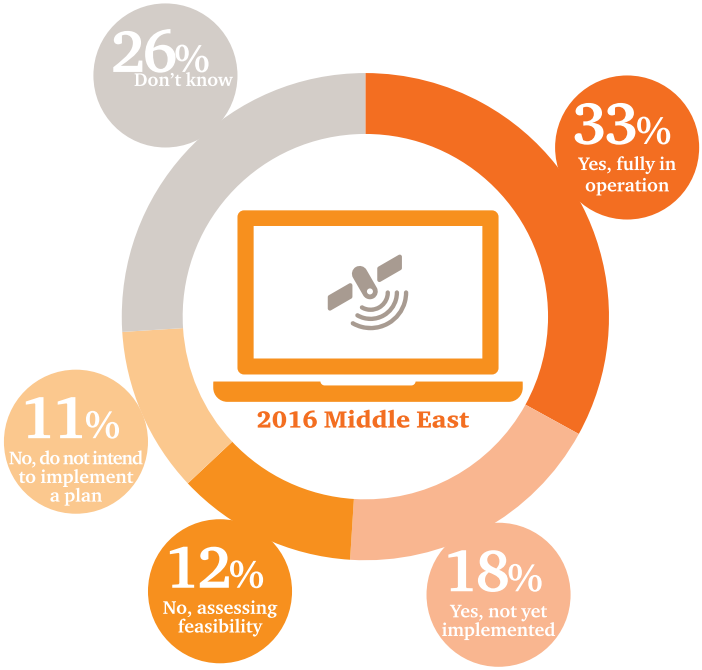
Tackling cybercrime also means managing and planning for it in the same way as any other business threat or potential disruption. Prevention is better than cure, but it's important to be properly prepared if an attack does happen. That requires detailed crisis planning, clear roles and responsibilities, regular and rigorous testing, and a cross-functional team ready to respond immediately. But at the moment only 33% of the region's respondents have operational plans in place with fully trained staff, and most of those people are from IT.

In other words, far too many Middle Eastern organisations are leaving first response to their IT teams without the support or involvement of senior leaders or other vital functions. Only 15% include Legal, 12% HR, and 12% a digital forensic investigator who is experienced in evidence collection and preservation techniques not commonly known by IT staff. IT staff in the region generally 'walk all over evidence' during a breach. This includes continuing to work on servers, failing to ensure logs are exported or backed up immediately, and omitting to create forensic images of the computer and Random Access Memory (RAM) where malware and viruses have been detected. By simply turning off a computer or server, there is a risk of losing what malware is doing to the computer, the network, or the organisation. An entire investigation could be jeopardised simply by running an anti-virus application, because the malware may be removed, or even destroy itself when it detects it's being investigated or cleaned. Staff mean well when they do this, but do not always understand the wider ramifications. This tallies with our own experience and anecdotal evidence, which suggests that both the understanding of cyber risks, and the level of proactive measures taken to deal with it, are lower in this region than elsewhere in the world.

To sum up, the key is preparedness – the ability to identify the potential for a cyber-attack, detect it when it does, preserve evidence to investigate and remediate, and do what you can to prevent further attacks as far as possible. And when an attack does happen, it's about fast, effective damage limitation.

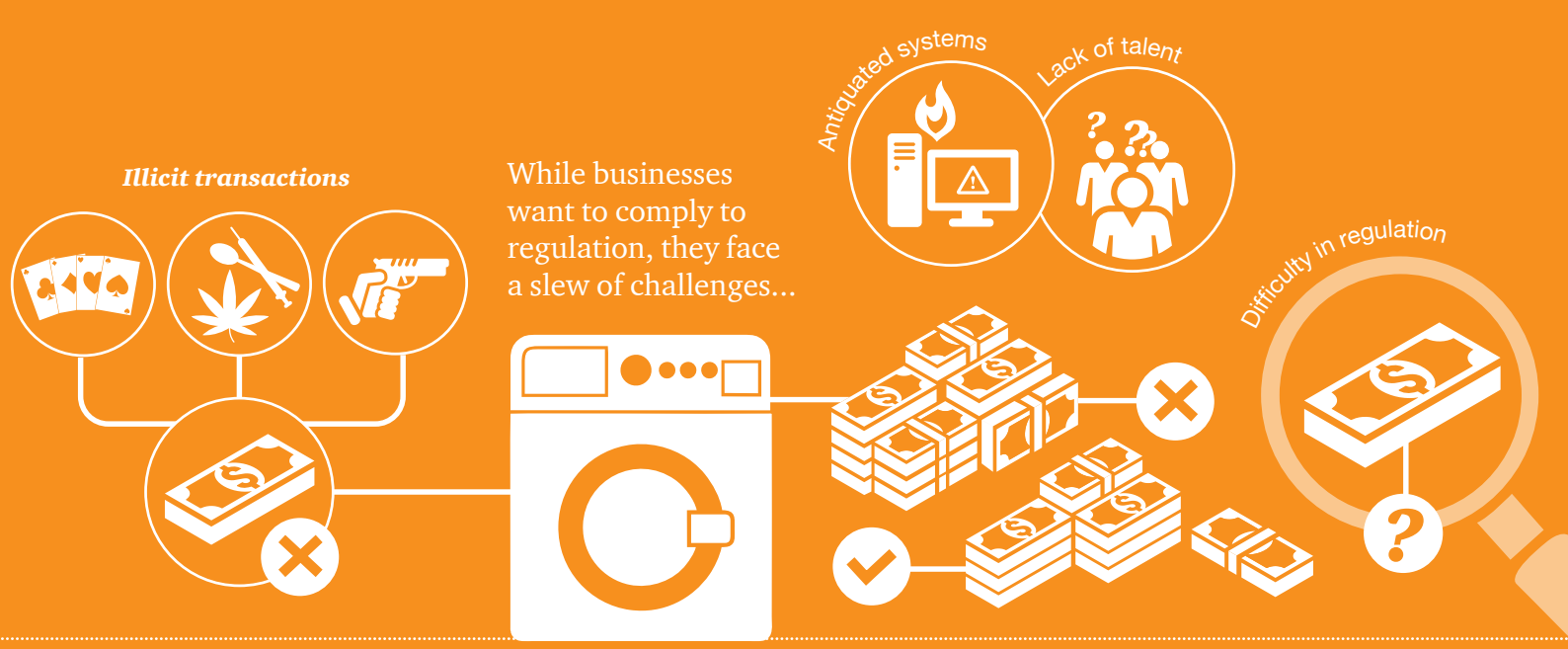
**Does your organisation have an incident response plan to deal with cyber attacks?**



**Has your organisation identified first responders who can mobilise quickly should a technology breach occur?**


# Anti-money laundering



# Money laundering destroys value

Money Laundering continues to be a significant problem across the world, with some estimates putting the value of illicit funds channelled through the financial services sector at up to $2 trillion[2].

Whether it's anti-money laundering (AML) or counter-terrorist financing (CFT), there's no question that regulation is getting tougher, more frequent, and more expensive to manage: global spending on AML compliance could top $8bn by 2017[3]. It's also costing more not to comply with it, with larger fines and a potentially disastrous impact on corporate reputations. This is reflected in the global survey results, with the two biggest challenges identified as the pace of regulatory change and the lack of skilled staff.

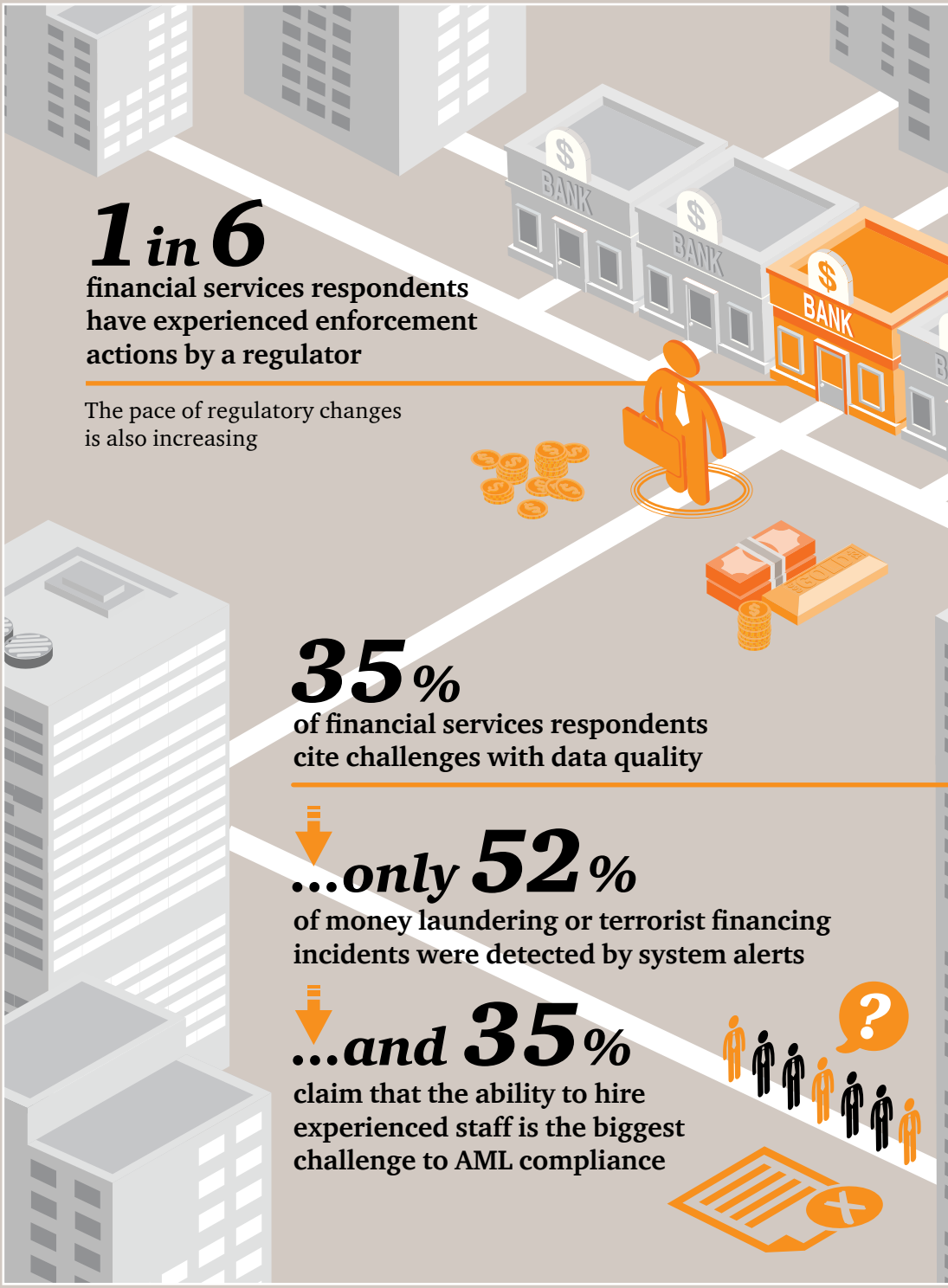
At its core, preventing these flows of funds is a human issue. We all want to prevent or detect the crimes that generate these illicit funds, or to identify those who use legitimately obtained money to finance criminal or terrorist activity. But we also recognise that the regulatory burden on the financial sector has become enormous, with the cost of compliance a concern for both global and regional financial services businesses.

The criminals and terrorists who try to use the financial sector to finance their activities are innovative, and new technologies make the problem more complicated every day. New online or app-based banking services, the emergence of alternative financial services providers, cryptocurrencies, and even online gaming technology, all create new challenges to monitoring and detection, and require compliance functions to think innovatively, and take as broad a perspective as possible, in assessing the risk of these crimes.

As the criminals get more innovative, the financial services sector is being forced to do the same – there are new techniques in areas like 'Know Your Client', greater sophistication in monitoring and screening technologies, and compliance functions are expected to broaden the scope of their traditional AML risk assessments and take a more holistic view.

2) From 'Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes' by the United Nations Office on Drugs and Crime © 2011 United Nations. Reprinted with the permission of the United Nations.
3) Statistics provided courtesy of WealthInsight

Heightened regulatory standards are driving sharp increases in enforcement action




**1 in 6**

**financial services respondents have experienced enforcement actions by a regulator**

The pace of regulatory changes is also increasing

**35%**

**of financial services respondents cite challenges with data quality**

**...only 52%**

**of money laundering or terrorist financing incidents were detected by system alerts**

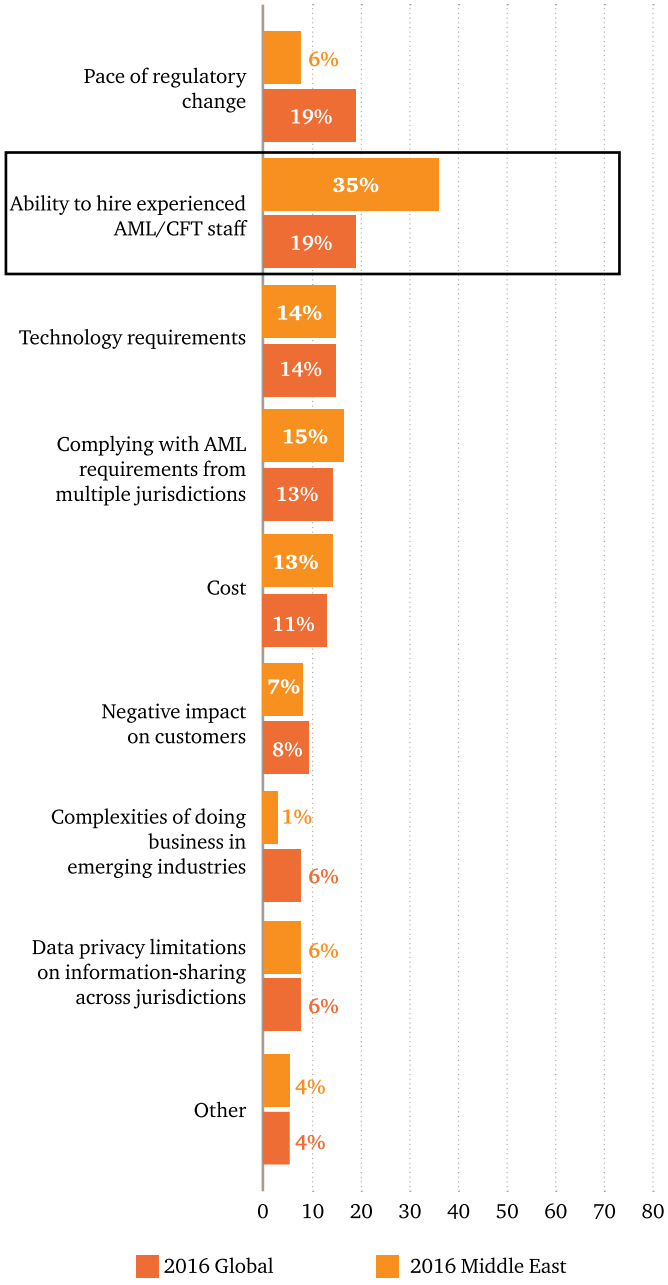
**...and 35%**

**claim that the ability to hire experienced staff is the biggest challenge to AML compliance**


More than 20%
of financial services firms have not conducted AML/CFT risk assessments across their global footprint
BANK
How would your organisation fare in the face of regulatory scrutiny?

The Middle East region has special challenges here, with an unusually wide range of both international banks and local banks with a global presence. There is also a very high level of money service businesses and cash transactions, combined with global trading hubs and a geographical proximity to unstable or sanctioned locations.

**Which of the following do you see as the most significant challenge/issue in relation to complying with your local AML/CFT requirements?**




What's interesting is the sharp discrepancy between the global and the Middle Eastern results in these two key areas. We recognise the difficulty in securing skilled resources in the region, and this clearly shows the increased demand from financial institutions to get the right people.

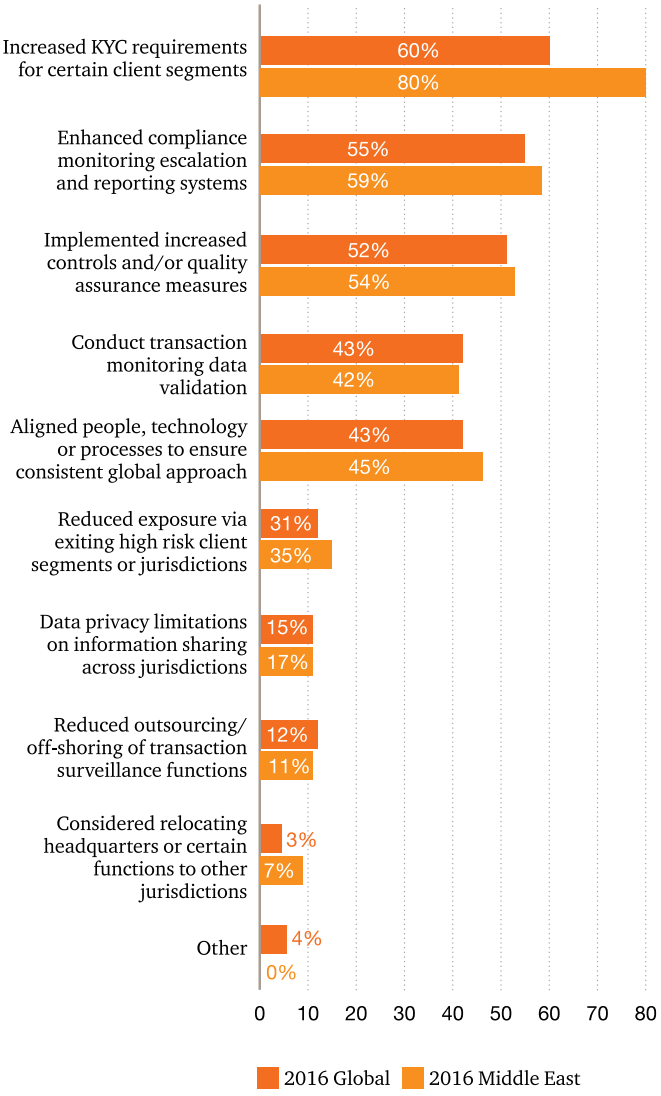
It's very surprising, however, that regional respondents aren't finding it harder to keep pace with regulation, though clearly the challenge of complying with multiple jurisdictions is very much top of mind. All the same, the results suggest to us that there may be a lack of understanding here, especially in relation to the impact of actions by overseas regulators in regions like the EU and US, and what these regulators are actually looking for.

The US, in particular, is driving the AML/CFT agenda across the world, and Middle Eastern companies will not be immune. For example, we have seen so-called 'de-risking', where US correspondent banks have ceased dealing with banks in the region where they believe the bank in question isn't complying with regulatory requirements. This has major implications for those banks' ability to offer services to local customers. 71% of Middle Eastern respondents have been through a regulatory inspection in the last two years (compared to 50% globally) proving that the authorities in the region are active, diligent, and poised to levy fines or impose sanctions, and that genuine local regulatory compliance deserves greater international recognition.

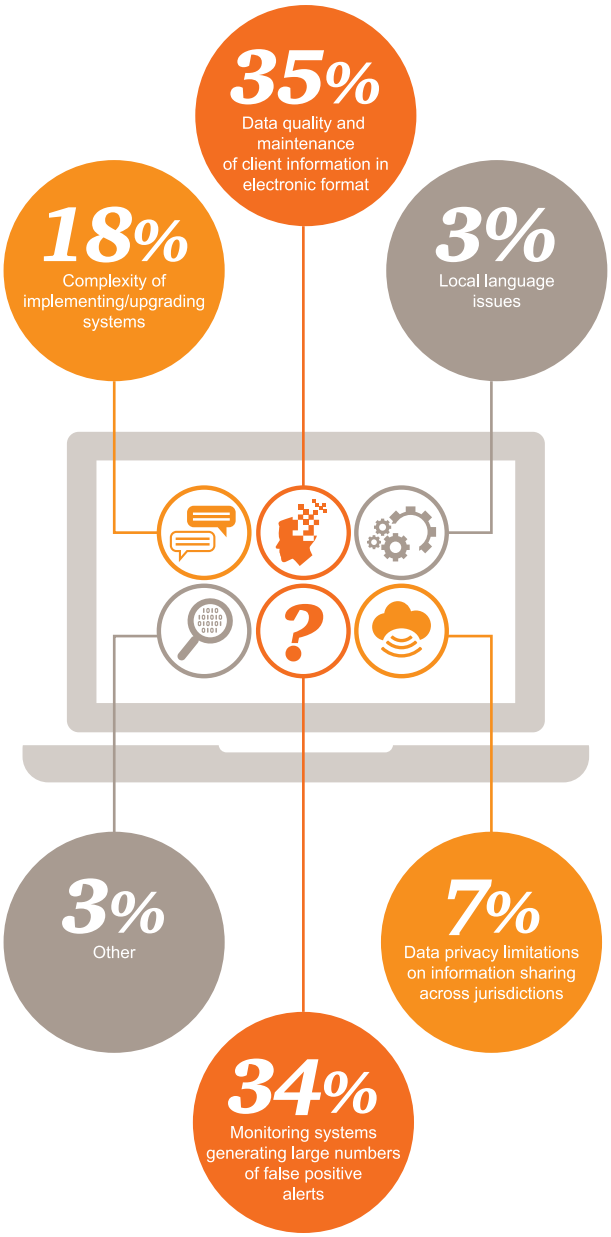
Middle Eastern respondents appear to be ahead of the curve in many areas of AML/CFT, and in the last two years 68% have hired additional resources, both in these areas and other roles related to regulation. But there may be a question-mark about how deep or extensive these new measures really are, and whether this has really enhanced the effectiveness of their AML/CFT mechanisms.

***Changes in international sanctions regimes have been a significant development in the region in recent years, and have a major impact on the financial services sector. Many of the most significant fines levied against global financial institutions in recent years were related to failings in sanctions compliance, and we expect this trend to continue. The message is clear: changes in sanctions regimes may create potential new opportunities for growth and expansion, but organisations need a detailed understanding of the new regime, and Boards of Directors need to tread extremely carefully.***

## Which of the following activities has your organisation implemented to reduce AML/CFT risks?




## Most significant challenges with respect to AML/CFT systems




The emphasis Middle Eastern companies are playing on 'Know Your Client' measures is very much on point. Whether you're a bank or another type of business, you need to know who you're dealing with. This has never been more important than it is now, with so much business being transacted remotely, with people you will never meet. But by doing business that way you are – in effect – putting your brand in their hands.

As in other areas of economic crime, data collection and analysis can play a hugely helpful role, both in monitoring and detecting potential AML or CFT activity. New digital infrastructure could cut costs and improve efficiency, but many banks are hampered by cumbersome unconnected legacy systems that are no longer fit for purpose, but are too expensive and difficult to change. 35% of respondents in the Middle East say data quality is an issue (as against 33% globally), 18% are struggling with upgrading or implementing systems (24% globally), and 34% have systems that generate large numbers of false positive alerts (23% globally).

There's one clear message from this year's Global Economic Crime Survey, which is as relevant to the Middle East as it is everywhere else in the world.

Money laundering and terrorist financing remain a significant threat to society, and have not diminished, even in light of the increased focus on financial crime regulation in the past decade. Regulatory expectations continue to grow, and financial institutions are at the front line of efforts to detect and prevent the financing of criminal activity.

Financial institutions in the Middle East will need to continue investing in reviewing their controls and ensuring their compliance efforts are comprehensive, holistic, and continuous. Failure to do this not only puts the organisation at risk, but potentially fails to prevent the underlying criminal activity that these controls are designed to prevent.

# Participation statistics

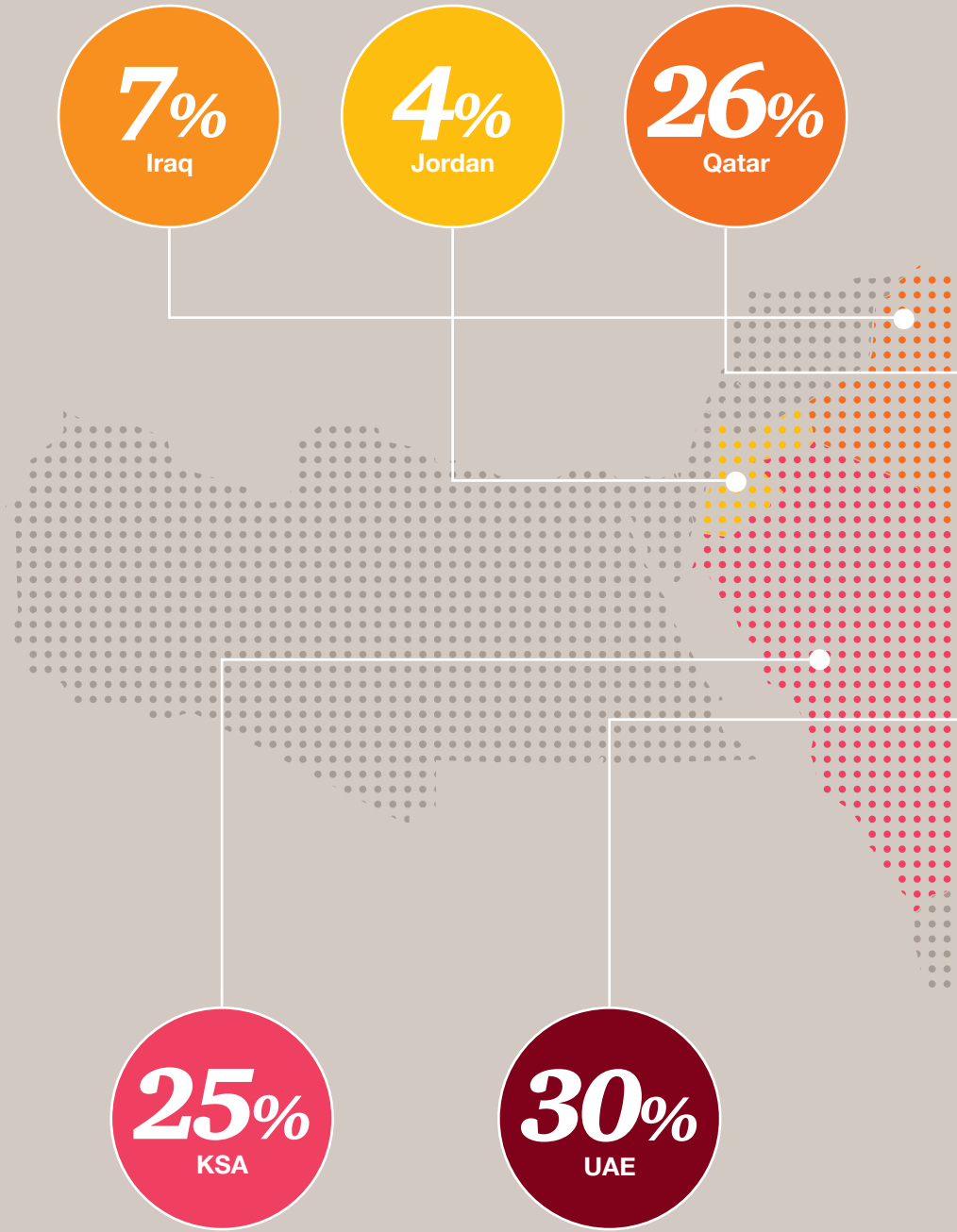
## Participation statistics

Over **290** completed surveys

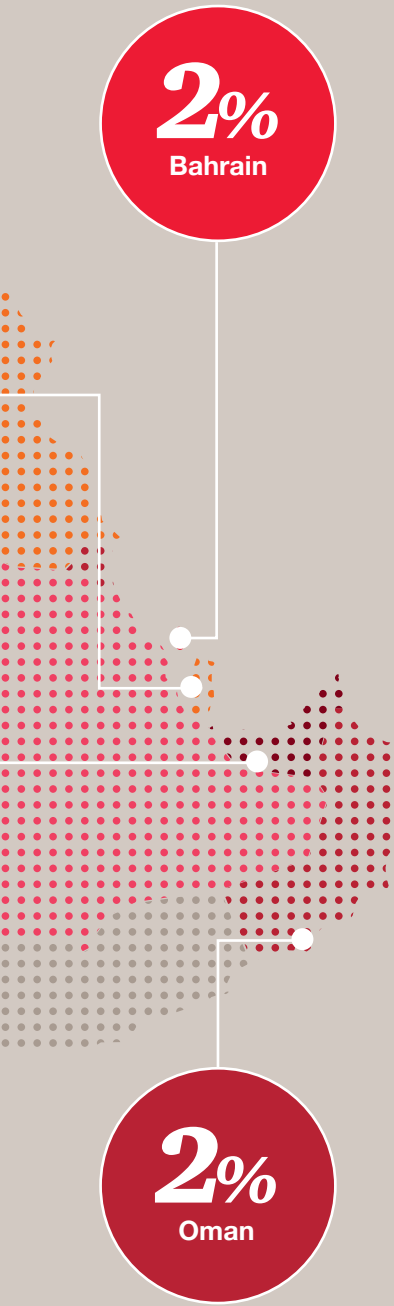
Across **12** countries

Surveyed in **2** different languages

## Participation by region



# Respondents





**65%**
of respondents were managing the Finance, Executive Management, Audit, Compliance and Risk Management Functions

**57%**
of respondents employed by organisations with more than 1,000 employees, with

**41%**
of these participants having more than 10,000 employees

**32%**
of the survey population represented Publicly Traded Companies, and

**60%**
of respondents were from multinational organisations

# Contacts


**Nick Robinson**
Middle East Forensic Services Leader
T: +971 (0) 4 304 3974
M: +971 (0) 50 899 2087
E: nick.e.robinson@ae.pwc.com

**John Wilkinson**
Middle East Regional Deals Leader; Senior Partner Forensic Services
T: +971 (0) 4 304 3538
M: +971 (0) 50 900 7491
E: john.d.wilkinson@ae.pwc.com

**Tareq Haddad**
Partner – Forensic Services
T: +966 (11) 211 0400 (ext. 1880)
M: +966 (0) 56 091 1113
E: tareq.haddad@sa.pwc.com

**Tania Fabiani**
Partner – Forensic Services
T: +971 (0) 2 694 6991 (ext. 2991)
M: +971 (0) 50 642 4483
E: tania.fabiani@ae.pwc.com

**Achraf El Zaim**
Partner – Forensic Services
T: +971 (0) 4 304 3132
M: +971 (0) 50 841 0383
E: achraf.elzaim@ae.pwc.com

**Mike Maddison**
Middle East Cybersecurity Leader
T: +971 (0) 4 304 3444
M: +971 (0) 56 683 8253
E: mike.maddison@ae.pwc.com


**Editorial Team**


**Muhammad Khurram N. Khan**
T: +971 (0) 4 304 3635
M: +971 (0) 50 900 9827
E: muhammad.k.khan@ae.pwc.com

**Rohan Shoaib**
T: +971 (0) 4 304 3705
M: +971 (0) 50 765 7044
Email: rohan.shoaib@ae.pwc.com

**Ismail Hussain**
T: +974 (0) 4 419 2733
M: +974 (0) 5 539 3997
E: ismail.hussain@qa.pwc.com

**PwC Middle East**

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

Established in the Middle East for 40 years, PwC has firms in Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Oman, the Palestinian territories, Qatar, Saudi Arabia and the United Arab Emirates, with around 4,000 people. (www.pwc.com/me).

Creative Design centre 11922016 CDC

***www.pwc.com/me/crimesurvey***