PwC Middle East Economic Crime Survey
February 2014

Economic Crime in the Arab World

21%
One in five Middle East organisations report being the victim of economic crime

5%
Only 5% of frauds were detected by routine Internal Audit

37%
More than one in three victims of economic crime reported incidents of cybercrime

38%
More than one third of Middle East respondents believe they will suffer procurement fraud in the next 2 years

pwc

www.pwc.com/me

According to 70% of CEOs surveyed, economic crime continues to be a major concern for organisations of all sizes, across all regions and in virtually every sector.

Table of contents

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 157 countries with close to 184,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more 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 2,700 people. (www.pwc.com/middle-east)

Foreword

We are pleased to present to you our second edition of the PwC Global Economic Crime Survey – Middle East Report. This survey provides the views of respondents from more than 230 organisations in nine Arab Countries making it one of the most comprehensive studies in the Middle East.

This report provides important insights into the trends of economic crime in the region. Economic crime is a risk that threatens economic development and impacts the welfare of peoples. Economic crime in the public sector impacts every aspect of daily life and hinders investment. It also threatens businesses by compromising their internal processes, eroding the integrity of employees, and tarnishing reputations that take long years to build.

In the past few years we have seen an increased focus by both the public and private sectors on fighting economic crime. Many governments have set up anti-corruption bodies tasked with reducing corruption in their countries by implementing proactive measures, reacting to incidents, or both. Although we have seen several good initiatives much more is still needed to build the capacity to fight economic crime and reduce it to much lower levels. On the other hand countries that have witnessed changes in ruling regimes have suffered from a deficit of controls which correspondingly increased the risk of economic crime.

A determined focus is needed by the incoming governments to combat economic crime, and to reinstate supervisory and control bodies at a national level.

In the private sector, we have been seeing an increased focus, particularly within large businesses, on building their fraud risk frameworks. Over 70% of the CEOs of some of the leading organisations in the Middle East who participated in PwC's Global CEO Survey [1] highlighted that they are concerned or extremely concerned about the risk of bribery and corruption. We have also noticed that businesses in the region are increasingly starting to realise that proper responses to incidents of economic crime, despite the short-term impact on employee morale, can act as an effective deterrence mechanism, helping in the longer term to set the proper tone in the organisation and preserve value.

This year we have made two particular themes the focus of our report. Our survey shows that cybercrime is now the second most reported type of economic crime in the region, hence we have devoted a section of our report to it. In addition, we focus on corruption which remains a pervasive risk to the region, both in terms of the level of incidents reported in our survey and the significance of the negative impact this creates inside and outside our borders.

We hope that you will find this report useful both as a reference point in the ongoing campaign against economic crime but also as a strategic tool to help you consider the economic crime risks which your organisations face, and to enhance your control mechanisms to prevent, detect and respond to economic crime.

We are very grateful to all the respondents and organisations that made this Middle East Report possible by taking the time to complete the survey.

John Wilkinson, Partner
Middle East Forensic Services Leader
Dubai – UAE

Tareq Haddad, Partner
Middle East Investigations Leader
Riyadh – KSA

[1] www.pwc.com/ceosurvey

The highlights

21%

Reported incidents of economic crime in the Middle East have declined. 21% of respondents in the 2014 survey suffered some form of economic crime, compared to 28% in 2011. This contrasts with the results of our global survey which saw an increase in reported incidents from 34% to 37% over the same period.

Asset misappropriation remains by far the most commonly reported type of economic crime followed by cybercrime and bribery and corruption.

Cybercrime is now the second most common form of economic crime reported, demonstrating the extent to which new technologies are creating opportunities for technologically sophisticated fraudsters.

More than half of the respondents believe that bribery and corruption is a significant risk to their organisation when doing business globally. 18% of respondents indicated that their organisation had been asked to pay a bribe, and 24% believed their organisation had lost out to a competitor who paid a bribe.

18% of respondents indicated that their organisation had been asked to pay a bribe

24% believed their organisation had lost out to a competitor who paid a bribe

This year's survey identified significant incidences of procurement and human resources fraud, each of which were reported by more than one third of those who reported suffering some form of economic crime.

Over 60% of respondents who reported fraud indicated that the perpetrators were internal staff, with nearly 90% of those indicating that 'opportunity' was the biggest factor contributing to this.

The profile of a fraudster has changed: whilst the majority of economic crime is still perpetrated by male, internal staff our 2014 survey shows the principle demographic is senior management staff aged 41-50, rather than middle management staff aged 31-40 as reported in 2011.

Respondents in the Financial Services sector reported that 60% of frauds suffered were perpetrated by external parties, significantly above the results for any other sector.

60% External

Regrettably 16% of economic crime in the Middle East is detected by chance, significantly above the global average of 7%, indicating a widespread lack of effective fraud detection methods in the Middle East.

The financial impact of economic crime remains high: 12% of respondents said that the direct financial impact on their business was greater than USD5 million in the last 24 months. Interestingly, the percentage of respondents who indicated that the financial impact was greater than USD 100 million increased to 6%, which is three times the global average.

The perceived non-financial impact of economic crime has changed. In our 2011 survey the greatest perceived impact was on the reputation or brand of the victim organisation. In our 2014 survey our respondents indicated that the greatest perceived impact was on employee morale.

More than 38% of respondents predicted that their organisation will suffer from some form of economic crime in the next 24 months.

Looking ahead, Middle East organisations are most concerned about procurement fraud, bribery and corruption and asset misappropriation. In our opinion all organisations must be concerned about cyber crime, which we expect to be a growing trend of criminality in the coming years.

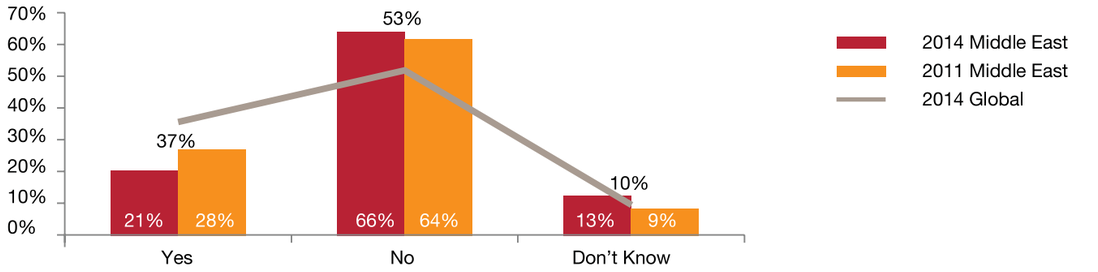
Economic crime in the Middle East
The big picture

The 2014 GECS confirms that economic crime remains a fundamental fact of life for organisations in all regions and in all industries. The worldwide incidence of reported economic crime is on the rise – 37% of respondents globally reported suffering some form of economic crime compared to 34% in the 2011 survey.

This global trend in reported frauds has always fluctuated, but in every survey in the 14 years since the PwC Global Economic Crime Survey was launched the figure has been at least 30%.

In the Middle East, however, the situation is different. Our 2011 Middle East report highlighted that 28% of respondents indicated that their organisations had reported incidents of economic crime – well below the global average. This year's report indicates that the rate of reported incidents of economic crime has dropped to 21%. Nonetheless, those organisations which reported economic crime experienced more types of economic crime than the global position. This could suggest that where economic crime is present it is more pervasive in Middle Eastern organisations than the global average.

Figure 1: % of respondents who suffered some form of economic crime

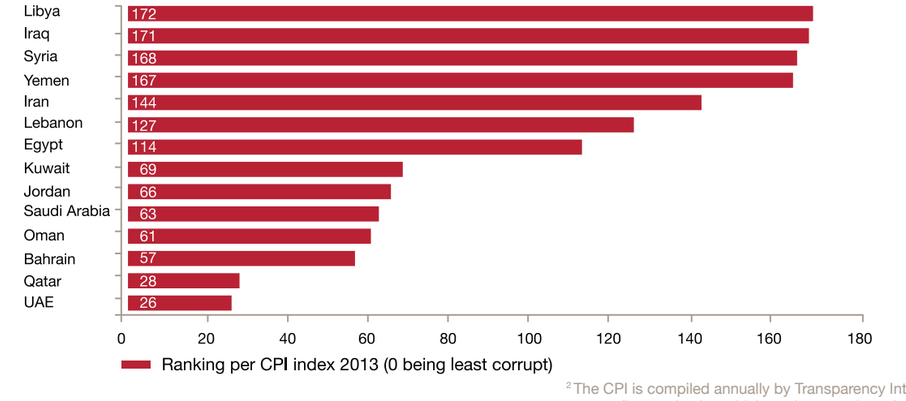


To put this into further context, the Middle East reported fewer incidents of economic crime in both the 2011 and 2014 surveys than any other region, with the nearest comparator being Asia Pacific, where the figure is 32%. This is despite the fact that several countries in the Middle East have scored poorly on Transparency International's Corruption Perceptions Index[2].

It is important to note that there is an element of undiscovered fraud that has to be taken into consideration when looking at these results. Alarmingly, 16% of cases of reported economic crime in the Middle East were discovered by accident. While the true level of undetected fraud is very difficult to measure, the strength and effectiveness of fraud detection mechanisms can assist in identifying more incidents of economic crime.

Furthermore, in performing our analysis a clear story has emerged. The extent to which organisations in the Middle East are actively taking steps to protect themselves from economic crime is also below the global average: fraud risk assessments are conducted less frequently than the global norm – 54% of our respondents indicated that they had performed some form of assessment in the past 24 months compared to a global average of 64%. In the absence of a robust fraud risk assessment adequate risk-based controls cannot be properly planned and implemented. This in turn leads to a lower than average rate of detection of economic crime from manageable internal controls such as internal audit (Middle East: 5%, Global: 12%), targeted fraud risk management controls (Middle East: 3%, Global: 11%) and structured data analysis (Middle East: 5%, Global: 9%).

Figure 2: Middle East country rankings, CPI index 2013



[2] The CPI is compiled annually by Transparency International, a non-profit organisation which tracks a number of corruption indices. Please refer to www.transparency.org

The big picture, therefore, is that while the level of reported economic crime has declined in the region, organisations throughout the Middle East should be doing more to implement tailored, fraud risk focused controls to identify and combat the current level of unreported economic crime.

In this report we analyse the types of economic crime suffered in our region and their impact in both financial and non-financial terms. We also highlight the profile of those reported to have perpetrated fraud and provide some practical guidance on what businesses can be doing to mitigate their risk.

Types of economic crime
Common themes, emerging threats

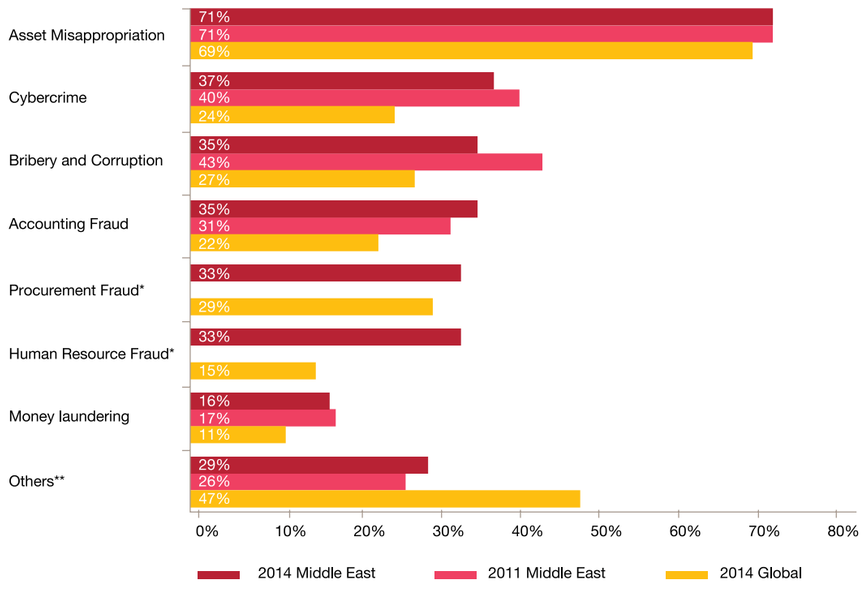
The results of the survey identified that 21% of respondents had suffered at least one instance of economic crime in their organisation. This rate of reported incidents is lower in the Middle East than anywhere else in the world, but the variety of crime suffered by those who did experience it in some form is consistently more varied than the global picture.

The survey showed that four types of economic crime remain most common: asset misappropriation (by a considerable margin), cybercrime, bribery and corruption and accounting fraud. In our 2014 survey accounting fraud, unlike any other type of reported economic crime, has increased compared to the results in 2011.

This year, to recognise our perception of their importance both globally and within the Middle East, we have separately identified two further categories in our survey: procurement fraud and human resource fraud. Our experience in the Middle East is that these two business processes are of particular concern to the C-suite, and it is interesting to observe the significant volume of respondents who experienced economic crime related to them.

The graph below provides further detail on the range of economic crime suffered.

Figure 3: Types of economic crime suffered



** represents category introduced in the current year's survey*
*** 'Others' includes IP infringement, tax fraud, insider dealing, mortgage fraud, anti-trust practices and espionage.*

Asset misappropriation remains the most commonly encountered crime by organisations globally and in the Middle East. This is not surprising: theft of assets is the simplest form of economic crime, requiring minimal technology. It is perhaps the category where 'opportunity' plays the most significant role, as explored further below.

Cybercrime ranks, for the first time, as the second most reported economic crime in the Middle East though globally it is in fourth position[3]. Recent sophisticated cyber attacks in the region, combined with an increase in concerns about cyber security at a governmental level, may have contributed to this increase. Unsurprisingly respondents perceive the greatest threat of cybercrime coming from outside their organisation.

Bribery and corruption remains a significant threat in the Middle East and globally. Headline news has showed us that this type of economic crime can have some of the most devastating impacts on organisations.

Accounting fraud has been more prevalent in the Middle East than globally over the last 24 months and, unlike the majority of other fraud types reported in our survey, has actually increased over that period. This could be a result of increasing pressure on management teams in the region to achieve ambitious financial and profitability targets.

As noted above, procurement fraud and human resource fraud are included in our survey as separate categories for the first time, and both are regularly suffered by Middle East respondents.

The high incidence of ***procurement fraud*** is interesting in the light of traditionally tight procurement tendering processes in this region. Our survey respondents who reported suffering from procurement fraud were asked to indicate which parts of the procurement cycle had experienced fraud in the past 24 months (see figure 4). The results indicate that current tender and vendor selection methods are not proving effective: a significant majority of respondents indicated that fraud is occurring in these stages of the procurement process, rather than at the payment stage.

Figure 4: Procurement fraud in the Middle East vs. Global

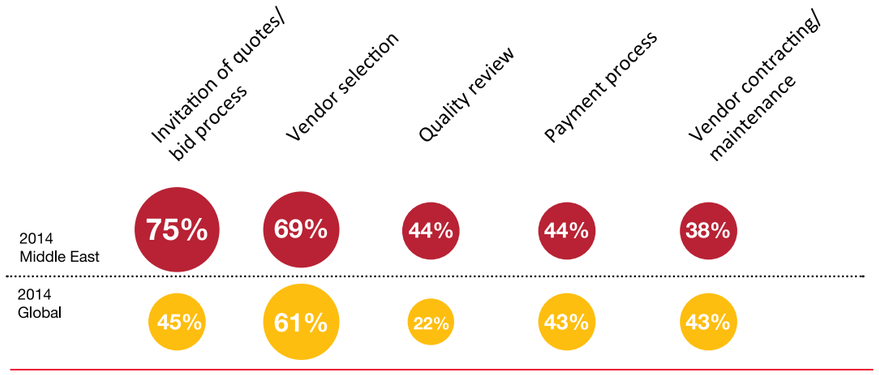
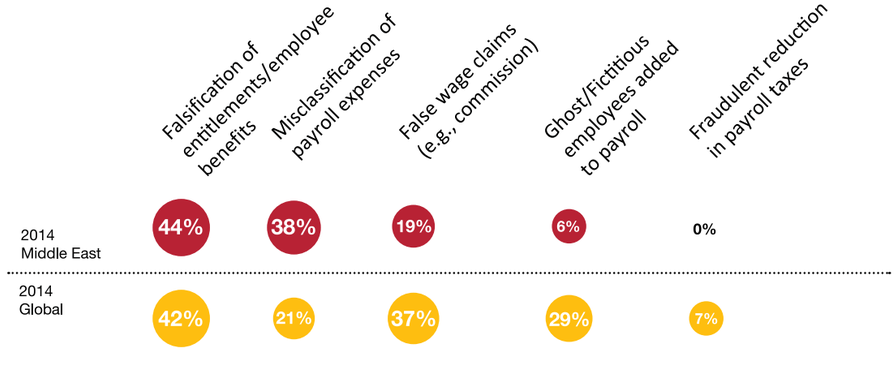


Figure 5: HR fraud in the Middle East vs. Global



[3] In the global survey asset misappropriation, procurement fraud and bribery and corruption are more commonly reported.

Combating procurement fraud – take preventative action

Even with strong controls in place, the procurement process can be vulnerable to fraud both from within the organisation and from outside.

In our experience, enhanced background screening of personnel involved in the tender process, coupled with thorough due diligence on bidding parties reduces the risk of procurement fraud. This will assist in identifying conflicts of interest, the decision makers' vulnerabilities and exposures, and the bidding parties' track record regarding fraud and corruption. Few organisations of any size undertake detailed checks of their bidders, and yet the evidence of previous misconduct may be easy to find. Due diligence of all parties need not be time consuming or costly, but will give companies more confidence in the ability of their tender board to make objective decisions and will expose bidders to an enhanced level of scrutiny.

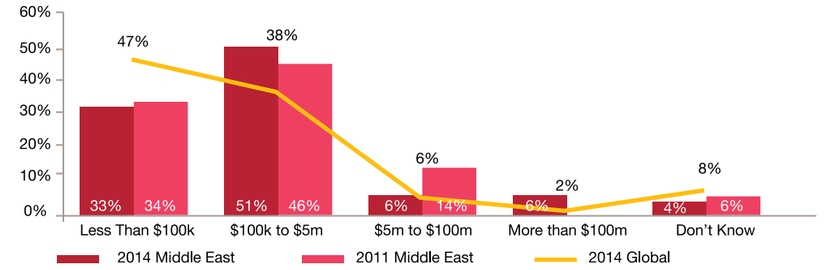
Courtenay Smith, Head of Corporate Intelligence, PwC

The damage caused by economic crime
A financial and non-financial cost

Of those who indicated that their organisations reported economic crime 51% said that the direct financial impact on their organisation of all frauds suffered in the last 24 months was between USD100,000 and 5,000,000, representing an increase from our last survey when the figure was 46%.

At the top end of the scale there are indications that incidents of economic crime of high financial impact increased where results show that 6% suffered total losses in excess of USD100 million. This indicates that the percentage of reported economic crimes in the Middle East where the financial losses are more than USD100 million is three times the global average.

Figure 6: The financial impact of economic crime



The case for more focus on prevention of fraud is therefore clearly proven from a financial perspective. But what about the non-financial impact that economic crime has on Middle East organisations?

Collateral damage

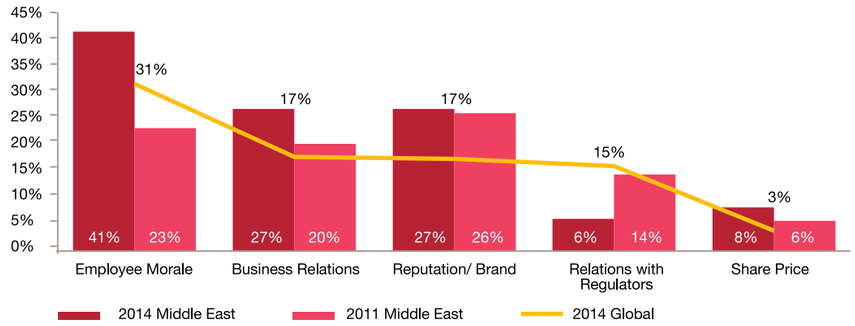
The fallout from fraud is not merely the direct cost. Our survey has highlighted the collateral damage suffered by Middle East organisations, taking into account a range of factors as shown at figure 7 below.

The change in these statistics since our last report is stark – Middle East organisations now consider damage to employee morale to be the number one collateral impact of suffering economic crime, ahead of more traditional 'commercial' indicators such as business relationships and brand reputation.

This is in line with the results from the global survey, but a significant shift from the Middle East results in 2011, when brand reputation was believed to be the most significant.

When evaluating the impact of economic crime it is important to consider the financial aspects in conjunction with the collateral damage which could have an impact on the organisation's productivity, ability to generate revenues, and ability to gain the trust of stakeholders including employees, business partners, shareholders and regulators.

Figure 7: The collateral impact of economic crime



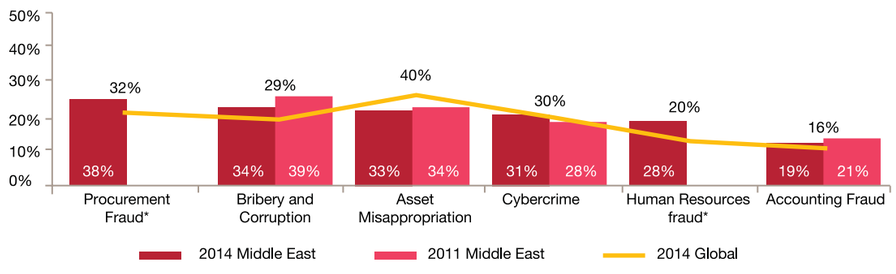
Looking to the future
Is economic crime on the rise?

Our survey asked respondents to consider the likelihood that their business would be a victim of economic crime in the future.

In our 2011 survey we indicated that the trend in reported incidents of economic crime was likely to rise: 28% of respondents at that time reported having suffered some form of economic crime in the past 24 months, but a significantly larger percentage thought the future looked bleak: 39% believed they were likely to suffer from at least one type of economic crime.

There is therefore a significant variance between the future expectations of respondents in 2011, where at least 39% predicted that their organisations would suffer from economic crime, and the level of reported incidents indicated in our 2014 survey of 21%. The results of the survey do not directly explain this variation: however the inherent nature of economic crime suggests that there will always be a level of incidents that will go undetected. It is also interesting to note that this year respondents again predict a further increase over the next 24 months, with 38% expecting their organisations to suffer from at least one type of economic crime.

Figure 8: Trends in Fraud Perception



** represents categories included in the current year survey*

In many cases, as shown by figure 8 above, these perceptions are greater than the global average.

37% of organisations who reported economic crime were victims of cybercrime in the last 24 months

Spotlight:
Cybercrime in the Middle East

The emerging threat

One of the key findings from this year's survey is that cybercrime is now the second most reported economic crime in the Middle East, rising from third in our 2011 survey.

Globally, 24% of respondents who suffered from some form of economic crime reported cybercrime, up one percentage point from 2011. In this region the burden is more significant, with 37% of victims of economic crime suffering from cybercrime.

According to a recent PwC survey[4], the most commonly occurring cyber threats in this region are to applications, systems and networks, but mobile devices, removable storage devices and data held by third parties are also at risk.

Recent high profile cases in the Middle East highlight the risks: in 2012 two of the region's largest oil and gas companies were reported to have been subject to cyber attacks which affected tens of thousands of individual computers, causing widespread disruption.

In 2012 and 2013 there were reported cybercrimes in the financial services sector across the region, in particular in the UAE, Oman and Lebanon.

One of the features of this developing threat is the speed with which attacks can be carried out – often subjecting the victims to significant financial, data or other losses before they even realise that an attack is in progress, diminishing the effectiveness of any response. Meanwhile the very technology on which the victim organisations rely becomes the tool used against them by the sophisticated criminal, whose identity can quickly be hidden, or changed.

The pace of technological change is also a factor. Sophisticated hacking groups are at the forefront of the development of new technology, and keeping pace with their methods is a significant challenge even at a governmental level.

Fundamentally in this region and globally businesses are struggling to understand, and keep pace with, cybercrime risks. Networks are not protected in a sophisticated manner designed to prevent access by sophisticated external parties.

Many local governments in the Middle East are now taking action, led by the UAE's Cyber Crimes Law 2012 and Saudi Arabia's 2012 Arab Cybercrime Agreement, in a bid to combat the growing threat.

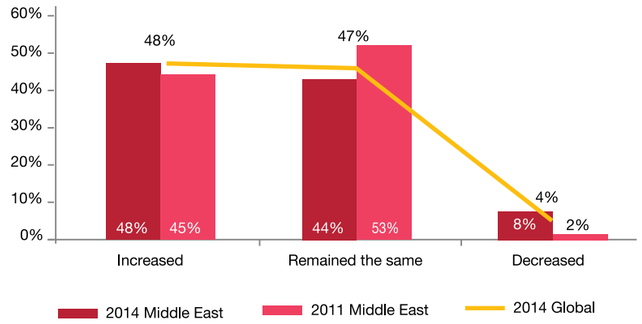
[4] www.pwc.com/security

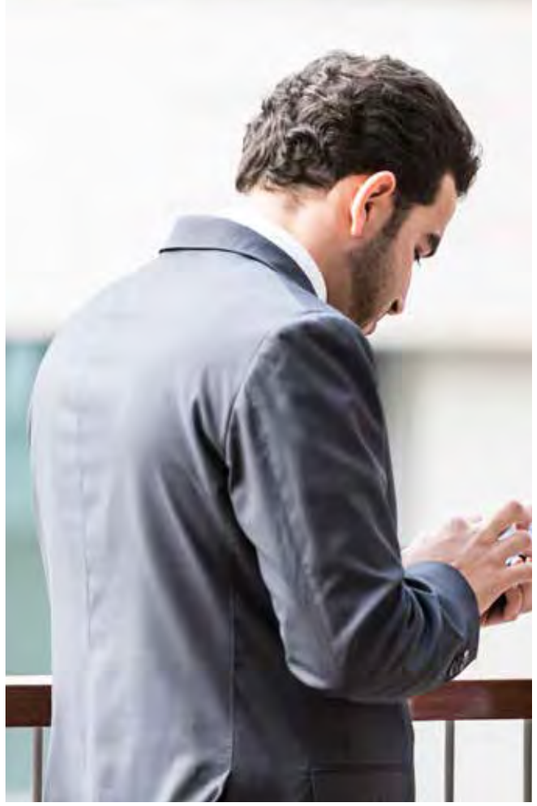
Perceptions

Our results show that cybercrime remains highly reported, both globally and in this region.

Perceptions are also changing. When asked whether their perception of the risks of cybercrime to their organisation had changed over the past 24 months 48% of our survey respondents indicated that the risk had increased, and 44% indicated that the risk has remained the same. Only 8% believed there had been a reduction in the risk from cybercrime.

Figure 9: Perception of cybercrime





The cost of cybercrime

Quantifying the true cost of cybercrime is notoriously difficult for a variety of reasons. Factors such as the opportunity cost of implementing cyber security frameworks, interruption to operations, loss of business, impact on safety systems, damage to brand or reputation, lost opportunities through decisions to avoid certain markets or products as a result of the perceived risk of cybercrime or the value of intangible assets lost to cybercrime, such as data or industrial methodologies, are near impossible to calculate.

Despite this inherent difficulty, we asked our survey respondents to estimate the cost of cybercrime to their business in the past 24 months. 35% indicated that they did not know what the actual cost of cybercrime was, whilst 40% responded that they believed there had been no financial loss from cybercrime.

These results highlight the scale of the problem. In many cases, those organisations reporting that they had suffered no financial loss may simply be unaware that they have been the victims of cybercrime in the first place or have not properly quantified the true business cost of the cyber attack. This is not unusual: the results from our global survey are exactly in line with the Middle East findings, with 40% of organisations globally reporting that they suffered no financial loss.

Of the Middle East respondents who did indicate the value of their losses from cybercrime 6% indicated that the loss was greater than USD1 million, with 2% reporting losses between USD5 million and USD100 million.

Taken together our results indicate that the true cost of cybercrime may be far more significant than reported.

Our experience has been that the level of sophistication employed by determined cyber criminals in the Middle East is as high as anywhere in the world. The persistency which hackers employ and the simple vulnerabilities they exploit present a real danger to Middle East organisations, whose staff may be the subject of cyber attacks and, knowingly or unknowingly, give away sensitive information or allow IT control breaches to occur. Combating this requires much broader planning than just IT security.

Dean Gilbert, Head of Forensic Technology, PwC

Where does the risk of cybercrime come from?

37% of respondents in the Middle East felt that the greatest cybercrime threat to their organisation came from outside their business, with only 9% believing the threat was internal.

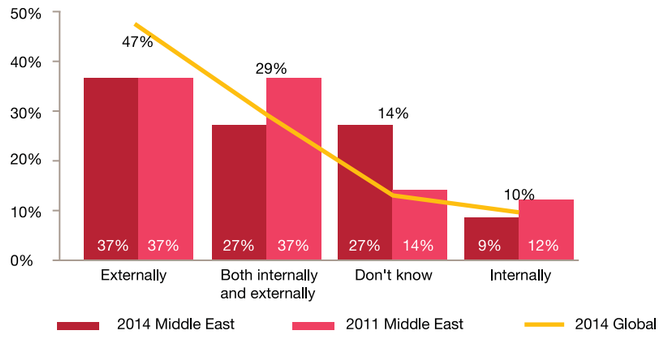
Whilst these results are not substantially different to the results from our 2011 survey, the increase in those who did not know where the greatest threat came from has increased dramatically from 14% in 2011 to 27% in 2014. In addition this figure is substantially higher than the global average of 14%. This suggests that more awareness about cybercrime and its impacts is needed in the Middle East.

What are Middle East organisations really worried about?

We asked our respondents what aspects of cybercrime they were most worried about. The results demonstrate a high level of concern about a range of factors with reputational damage, financial loss, disruption to their services, theft of Intellectual Property and theft of personal information all being concerns for more than 80% of all survey respondents.

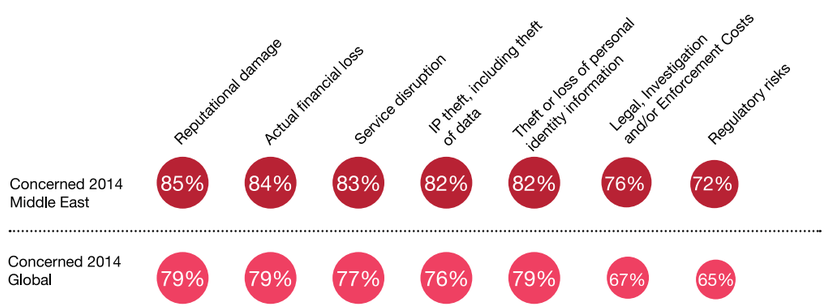
Our results also indicate that the level of concern is greater in the Middle East than globally, with respondents in this region expressing greater worry about every category of damage from cybercrime than the global average.

Figure 10: Greatest threat of cybercrime



Interestingly, respondents in the Middle East were least concerned with the regulatory risks and cost associated with legal support, investigation, and enforcement as a result of cybercrime.

Figure 11 : What keeps organisations awake?



Taking practical action – what can be done to combat the risk?

- **Get the C-Suite involved** – the CEO and the Board need to be aware of the risks of cybercrime and how these can influence strategic business decisions.
- **Look at how prepared the organisation is for cybercrime** – unlike traditional economic crime, cybercrime is fast-paced and technologically advanced, which means the organisation needs to be prepared to continually adapt.
- **Set up a cyber incident response team that can act and adapt quickly** – the organisation can then track and assess risks and deal with an incident as soon as it is identified.
- **Fight fire with fire** – recruit people with the right skills and experience: expertise is key to understanding the threat and taking decisive action if an attack is detected.
- **Take a tougher and clearer stance on cybercrime** – the organisation should show it means business by taking legal action against cybercriminals where possible.
- **Consult with others** – sharing knowledge of current cyber threats with others in the industry can help to provide early warnings of new developments.

35% of organisations who reported economic crime were victims of Bribery and corruption in the last 24 months

Spotlight: Bribery and corruption

35% of those respondents who indicated that their organisation had been the victim of economic crime had experienced corruption at some point in the survey period, making it the third most common crime suffered. This rate is significantly higher than the global rate of 27%.

When we asked about how the next 24 months look, **over one third of respondents in the Middle East predicted that their organisations would face bribery and corruption** issues in the next 24 months. It therefore remains a real risk.

While bribery and corruption was not the most common form of crime reported, of all the types of fraud covered in our survey it may pose the greatest threat to business both in the Middle East and globally. Cases of bribery and corruption reaching headline news indicate that the financial costs and collateral damage caused by incidences of bribery and corruption can be the most significant amongst the different types of economic crime. Governments, as well as commercial organisations in the Middle East are realising the increasing importance of fighting corruption.

At the public sector level several Governments in the Middle East region have established bodies mandated to lead the fight against corruption and bribery. Such organisations include the Abu Dhabi Accountability Authority in Abu Dhabi, the National Anti-Corruption Commission (Nazaha) in Saudi Arabia, the Jordan Anti-Corruption Commission in Jordan, the Anti-Corruption Authority in Kuwait and the Administrative Control and Transparency Authority in Qatar.

While many positive steps have already been taken by these bodies many are still in the early stages of development. Much work still remains to enable these organisations to effectively fight economic crime and reduce it to an acceptable level. Political will at the highest levels within Government is key to the success of these organisations.

On the other hand we have seen that businesses are starting to realise that more efforts are needed to fight corruption and to ensure that their business is driven by **innovation, competitiveness and efficiency.** This is particularly evident in larger organisations who are investing in enhancing and building their fraud risk management functions. We have seen several organisations and sovereign wealth funds conduct fraud risk assessments and design controls to specifically address corruption risks together with other types of fraud. We have also seen an increased awareness within boards of directors and audit committees about their responsibility to deal with the issues of corruption and bribery and launch objective and independent investigations where required.

Legislation and enforcement at a national and international level remain important factors in the fight against bribery and corruption. To date the US Foreign Corrupt Practices Act has already had an impact on businesses in the Middle East, though the UK Bribery Act has not yet had such a significant effect in the region.

At a national level, legislation and enforcement by Governments in the Middle East still require enhancement.

What action should organisations take to prevent bribery and corruption?

The UK Bribery Act of 2010 sets out six principles that may serve as a guide for commercial organisations in the Middle East who wish to prevent bribery being committed on their behalf. These are helpful guidance to any organisation seeking to better control the risk of bribery, and not exclusive to those subject to the UK Bribery Act.

1. **Proportionate procedures** - A commercial organisation's procedures to prevent bribery by persons associated with it are proportionate to the bribery risks it faces and to the nature, scale and complexity of the commercial organisation's activities. They should be clear, practical, accessible, effectively implemented and enforced.
2. **Top level commitment** - The top-level management of a commercial organisation (be it a board of directors, the owners or any other equivalent body or person) are committed to preventing bribery by persons associated with it. They foster a culture within the organisation in which bribery is never acceptable.
3. **Risk assessment** - The commercial organisation assesses the nature and extent of its exposure to potential external and internal risks of bribery on its behalf by persons associated with it. The assessment is periodic, informed and documented.
4. **Due diligence** - The commercial organisation applies due diligence procedures, taking a proportionate and risk based approach, in respect of persons who perform or will perform services for or on behalf of the organisation, in order to mitigate identified bribery risks.
5. **Communication (including training)** - The commercial organisation seeks to ensure that its bribery prevention policies and procedures are embedded and understood throughout the organisation through internal and external communication, including training, that is proportionate to the risks it faces.
6. **Monitoring and review** - The commercial organisation monitors and reviews procedures designed to prevent bribery by persons associated with it and makes improvements where necessary.

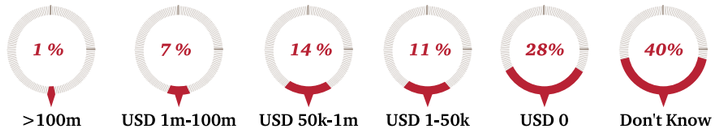
Perception and impact of bribery and corruption

Consistent with the global average, more than half of the Middle East respondents said that they perceived corruption to be a significant risk to their organisation when doing business.

Two fifths of Middle East respondents said that the most severe impact that corruption had on their organisation was financial loss followed by damage to corporate reputation (27%). Globally however, 36% perceived damage to corporate reputation to have severe impact followed by financial losses (28%).

In the case of financial loss 7% of Middle East organisations and 4% of global organisations have lost between USD one million and USD100 million, with 1% in the Middle East losing over USD100 million. Surprisingly, 40% of organisations in the Middle East and 34% organisations globally are unaware of the amounts lost through corruption.

Figure 12: Financial losses suffered through instances of bribery and corruption



When asked if organisations had been asked to pay a bribe, nearly one fifth answered positively and nearly one quarter felt their organisation had lost an opportunity due to a competitor paying a bribe.

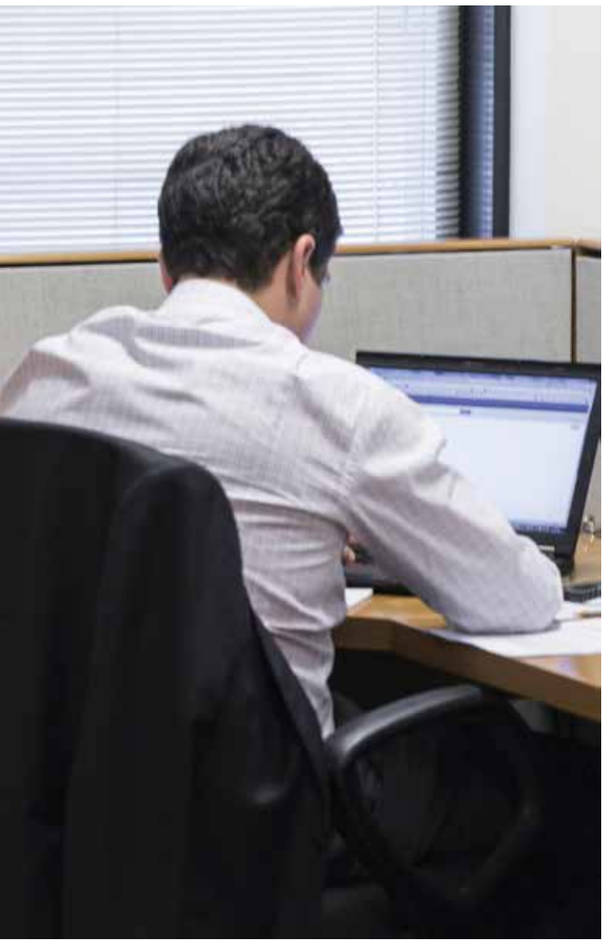


Figure 13: Instances where organisation lost to a competitor

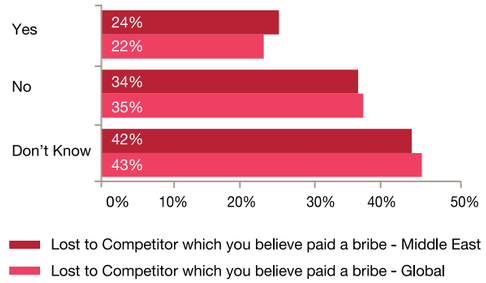
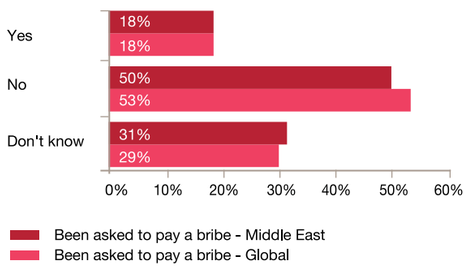


Figure 14: Instances where organisations were asked to pay a bribe



Know your enemy
Profile of a fraudster

As in our last survey we asked respondents who faced economic crime to profile the perpetrators of the most significant economic crimes impacting their organisation in the past 24 months.

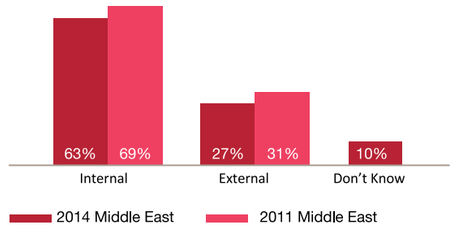
The enemy in plain sight

A large proportion of the Middle East respondents (63%) said that the perpetrators of fraud were from among their own staff. This is higher than the global average of 56% but lower than the results of our 2011 survey, perhaps reflecting the emerging threat of cybercrime and money laundering, which are mainly associated with fraudsters from outside the business.

Interestingly, the profile of the perpetrator has changed from our last report in 2011. The typical fraudster in our last report was internal to the organisation, male, between the ages of 31-40 and in a middle management position with a tenure of 3 – 5 years in the organisation.

The most prevalent profile of a perpetrator in our current survey remains an internal staff member and male but is viewed as now most likely to be in a senior management position and aged between 41-50 with more than ten years in the organisation. They are typically educated to degree level or higher.

Figure 15: Type of perpetrator



Profile of the internal fraudster

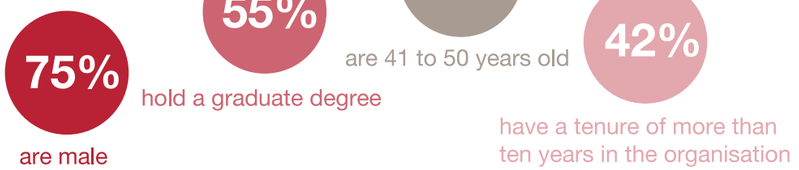


Figure 16: Profile of the external fraudster

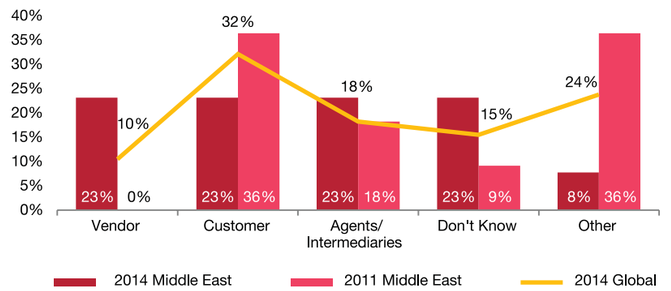
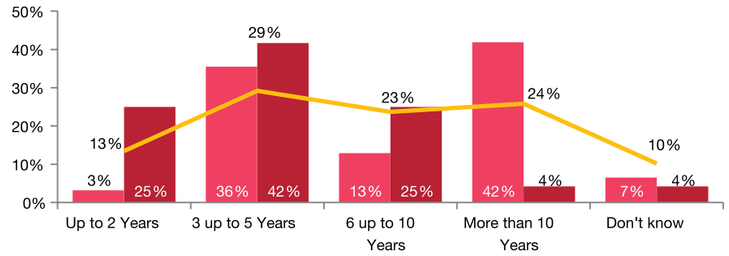
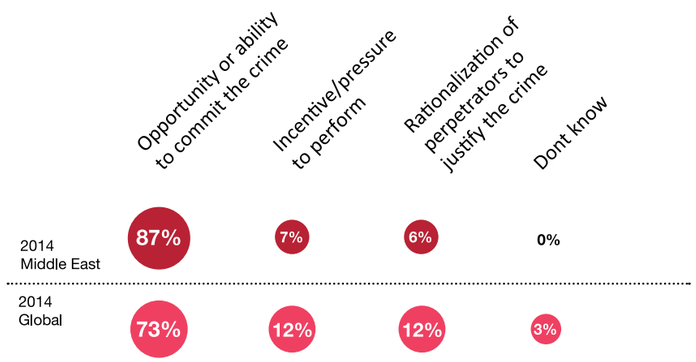


Figure 17: Length of service



We also asked our respondents to identify the factor that they believed had contributed most to economic crime within their orgnisation. Repondents overwhelmingly identified opportunity as the number one factor.

Figure 18: Factors for economic crime by internal fraudsters



Notwithstanding the individual demographic profile, the fact that perpetrators are mostly internal to the organisation is not surprising – given their greater level of knowledge over the organisations controls – but it should be considered an opportunity. Addressing the weaknesses in internal control which the internal perpetrator can exploit is one area over which management can have the most significant impact.

There are, however, exceptions to this rule. The financial services industry globally reports the inverse statistic – almost 60% of perpetrators are external.

In our Middle East survey 20% of respondents were from the financial services industry. One key driver is the risk faced by this industry from money laundering – almost universally a fraud perpetrated by external parties, in this case customers. Here, the results from the Middle East exceed the global average: 16% of respondents indicated they had experienced money laundering, compared to 11% globally.

Limiting the damage

Prevention and detection of economic crime

What can be done to detect an economic 'crime in progress'? Or better yet, how can it be prevented? Whilst there remains no sure way of eliminating fraud, the risk can be managed and reduced through effective controls.

Prevention

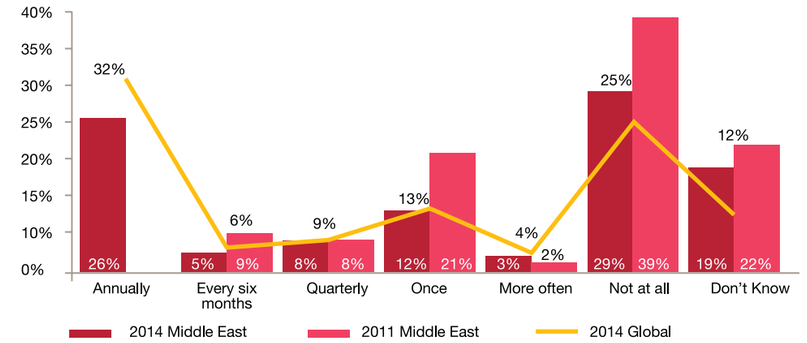
Preventing economic crime requires a clear understanding of what it is that needs to be prevented. A simple concept to grasp, but the only way to design effective anti-fraud controls is to conduct an assessment of the fraud threats that the business faces.

We asked our survey participants whether their businesses conducted fraud risk assessments in the past 24 months.

Only 42% of Middle East respondents indicated that their organisation conducted an assessment at least annually and 48% either did not conduct one at all or were not aware whether one had been conducted. As in our previous survey these results are substantially below the rest of the world, where reported incidents are noticeably higher – 51% of global respondents indicated that their organisation conducted a fraud risk assessment at least annually.

We also asked participants what the reasons were for not performing an assessment. One third of those who did not conduct one responded that there was a perceived lack of value from the process, highlighting the need for better education and awareness within organisations of the need for targeted fraud prevention.

Figure 19: Frequency of fraud risk assessment

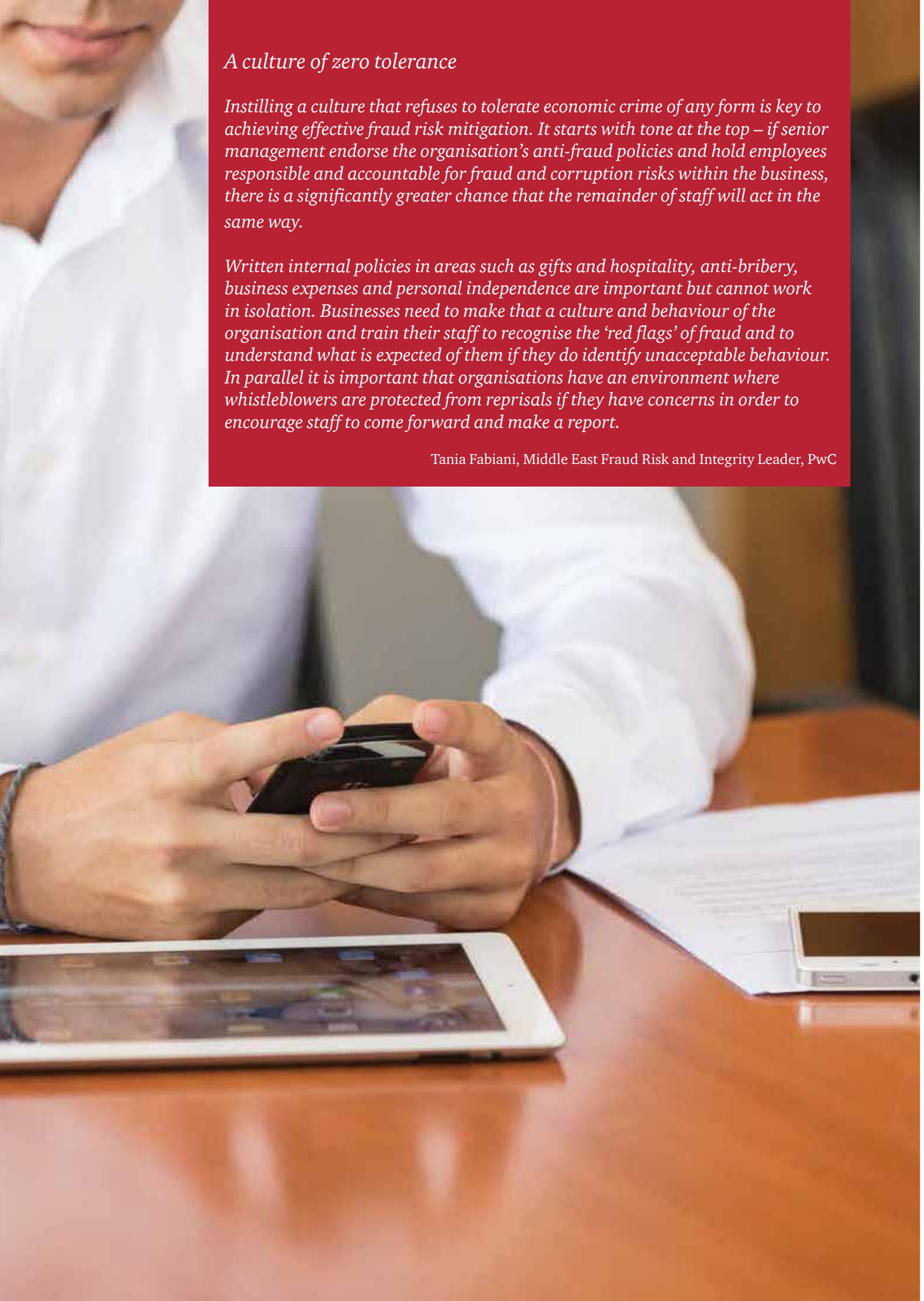


Note: There is no comparative figure for 2011 for fraud risk assessment conducted "annually"

In our view, the fact that the level of fraud risk assessments conducted in the Middle East lags behind the rest of the world, whilst reported incidents are significantly lower than the global average is an indication of the link between conducting fraud risk assessments on a regular basis and the detection of economic crime through focused controls when it occurs.

An effective fraud risk assessment considers factors from all angles:

- **Internal**: What controls does the business already have in place, are they tested and robust? Does the assessment cover all areas of the business? What influence does organisational culture and tone at the top exert on the fraud environment? What policies and procedures exist, and what level of training do staff, including internal audit, have in preventing and detecting fraud?
- **External**: Does the business operate in any high risk jurisdictions? Which counterparties does the business trade with, and do they have any history of fraudulent or corrupt practices? What is the regulatory and law enforcement landscape like? What are the risks from cyber attacks? What are the common issues being faced by the industry in relation to fraud?
- **The past**: Has the business suffered fraud in the past, and were lessons properly learned and controls tightened? Has there been a history of fraud schemes in the relevant industry from which lessons can still be learned?
- **The future**: Is the business about to enter new markets? Are new staff, new products and new business processes forecast in the next 12 months?



A culture of zero tolerance

Instilling a culture that refuses to tolerate economic crime of any form is key to achieving effective fraud risk mitigation. It starts with tone at the top – if senior management endorse the organisation's anti-fraud policies and hold employees responsible and accountable for fraud and corruption risks within the business, there is a significantly greater chance that the remainder of staff will act in the same way.

Written internal policies in areas such as gifts and hospitality, anti-bribery, business expenses and personal independence are important but cannot work in isolation. Businesses need to make that a culture and behaviour of the organisation and train their staff to recognise the 'red flags' of fraud and to understand what is expected of them if they do identify unacceptable behaviour. In parallel it is important that organisations have an environment where whistleblowers are protected from reprisals if they have concerns in order to encourage staff to come forward and make a report.

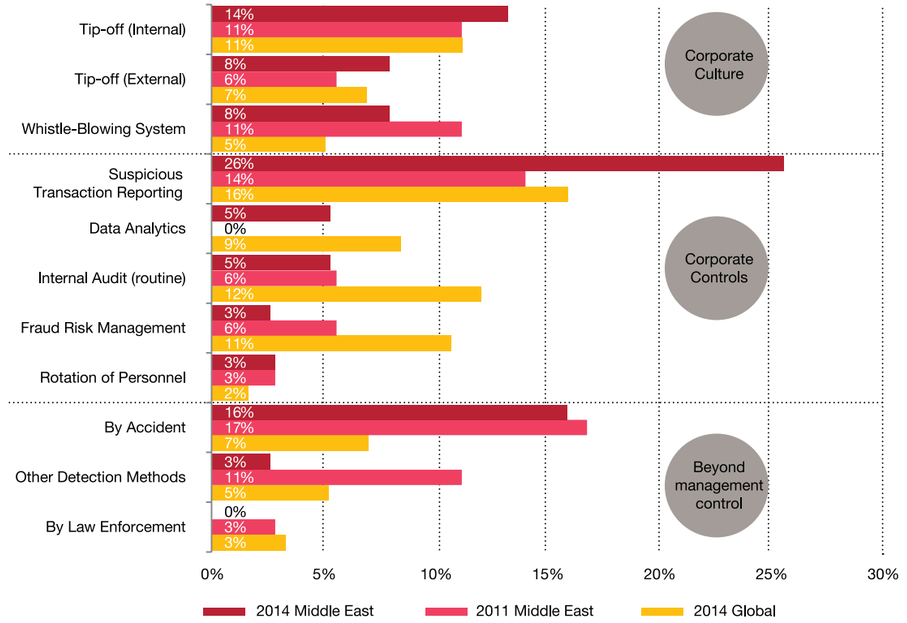
Tania Fabiani, Middle East Fraud Risk and Integrity Leader, PwC

Detection

Detection methods can broadly be grouped into three categories: corporate culture, corporate controls, and 'beyond management control'. As discussed earlier, 63% of our survey respondents indicated that frauds were most likely to be perpetrated by internal employees – providing an opportunity to directly target fraud risk through reinforcement of corporate culture and controls.

Figure 20 below details the method by which the major fraud at reporting organisations was detected.

Figure 20 : Detection of fraud



Corporate controls – more work is needed

Throughout our report we have highlighted the need for Middle East organisations to improve their focus on fraud risk management, principally through the establishment or enhancement of fraud risk assessments to improve the extent to which corporate controls target key fraud risks.

The methods by which frauds are detected reinforce this message: 16% of frauds are detected by accident, more than twice the average globally. Whilst it is pleasing to note that this percentage has decreased by one point from our 2011 survey, there is still real need for improvement.

Figure 20 above shows those methods of fraud detection which are having the greatest impact on the detection of major frauds.

Globally internal audit, fraud risk management techniques and data analytics – key components of corporate anti-fraud culture - are much more successful at detecting major frauds than in the Middle East. This highlights the real need for organisations in this region to focus on improving their internal anti-fraud controls.

Focus on corporate culture - whistleblowing

Methods of fraud detection which rely on corporate culture in large part involve the readiness of the individual employee or counterparty to recognise and report questionable behaviour when they see it. Rather than relying on tip-offs management can provide a ready route for reporting through the establishment of an effective and accessible whistleblowing mechanism.

In our survey we asked respondents about the existence and effectiveness of whistleblowing mechanisms in their own organisations.

Despite the decline in whistleblowing as the method by which the major frauds in our respondent's organisations were detected, over 50% indicated that they had a whistleblowing hotline in place and 56% of those said that their mechanism was effective or very effective (global: 50%). Middle East respondents were therefore more positive about the effectiveness of whistleblowing than the global average.

In this region 56% of our respondents said that their whistleblowing hotline had been used in the past 24 months compared to 50% globally, with 8% indicating it had been used more than 50 times over that period.

This presents an interesting contrast: Middle East respondents report higher usage of whistleblowing than the global average and are more positive about its effectiveness in their businesses, yet the number of major frauds detected in this way is falling, and is lower than the global average.

Figure 21: Organisations and whistleblower mechanism

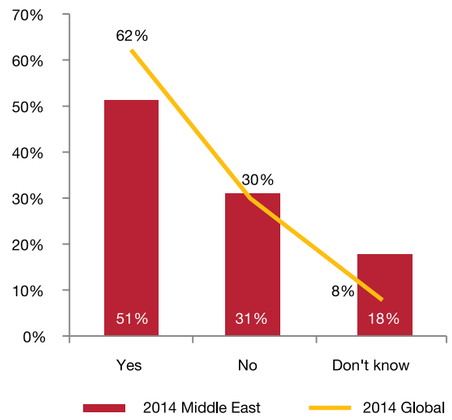
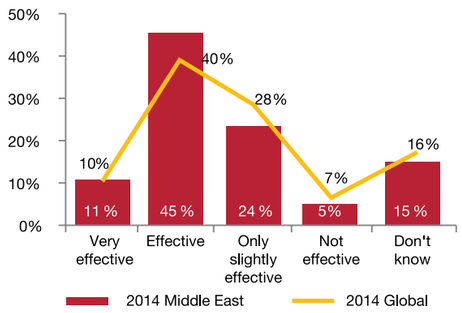


Figure 22: Effectiveness of whistleblowing mechanisms

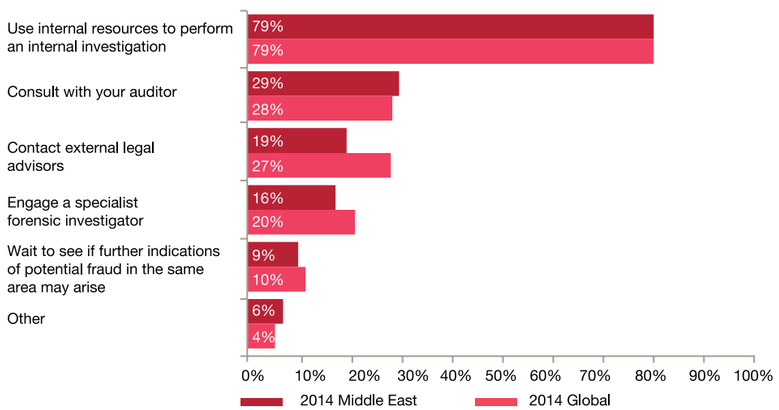


When a fraud is detected, what action are Middle East organisations most likely to take?

In this year's survey we asked our participants to outline their fraud responses where a potential fraud is identified. Almost four fifths of Middle East organisations said that they would use their internal resources to conduct an investigation, exactly in line with the global average.

Although 29% indicated that they would consult with their auditor, fewer respondents than the global average indicated that they would engage a specialist external party, either a specialist forensic investigator or their legal advisers, despite the benefits that a specialist resource might be able to provide.

Figure 23: Actions taken when potential fraud is identified



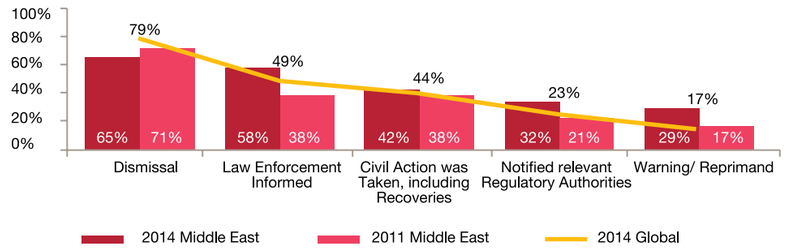
Taking action

Taking decisive action against the perpetrators of economic crime helps to reinforce the message that fraud is not tolerated, and underlines a strong anti-fraud culture.

Our survey has assessed the action taken by Middle East organisations in response to economic crime. Consistent with our 2011 survey, where fraud has been detected the response has been decisive and aggressive whether the perpetrator is internal or external.

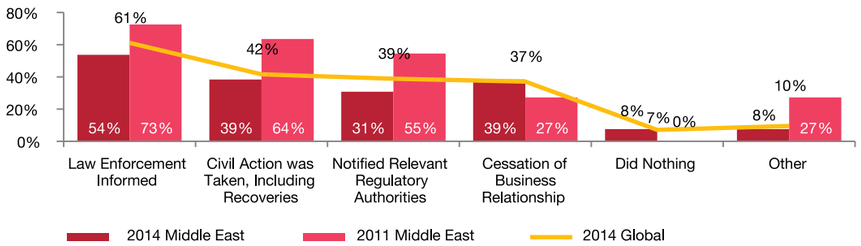
In response to incidents of ***internal*** fraud 65% of respondents indicated that they dismissed the perpetrators, 58% of the respondents notified law enforcement agencies and 42% took civil action.

Figure 24 : Actions taken against internal perpetrator



Our survey results show that external fraudsters represented approximately one quarter of all perpetrators of frauds detected. In these cases the majority of Middle East respondents informed law enforcement (54%), took civil action against the perpetrators (39%), ceased their business relationships (39%) and notified the relevant regulatory authorities (31%). Only 8% took no action at all.

Figure 25: Actions taken against external perpetrator



Methodology and acknowledgements

About the survey

We carried out our seventh Global Economic Crime Survey between August 2013 and February 2014. The survey had four sections:

- General profiling questions
- Comparative questions looking at what economic crime organisations had experienced
- Cybercrime fraud threats
- Corruption/bribery, money laundering and competition law/anti-trust law

Of the total number of respondents, 50% were senior executives in their respective organisations, 35% represented listed companies and 54% represented organisations with more than 1,000 employees.

The 2014 Global Economic Crime Survey: Middle East was completed by 232 respondents from nine countries in the region. Comparative indicators for respondents in the Middle East are provided below.

Job titles of participants

	% respondents
Manager	34
Chief Financial Officer/Treasurer/Controller	21
Head of Department	13
Chief Executive Officer/President/Managing Director	9
Senior Vice President/Vice President/Director	7
Other C-level Executive	7
Head of Business Unit	4
Board Member	1
Chief Security Officer	1
Don't know	2

Function (main responsibility) of participants in the organisations

	% respondents
Finance	32
Audit	16
Executive management	11
Advisory/Consultancy	11
Compliance	7
Marketing and sales	5
Other (please specify)	5
Risk management	4
Information technology	2
Legal	2
Operations and production	2
Security	1
Customer service	1
Human resources	1
Research and development	1

Participating organisation types

	% respondents
Private	52
Listed on a stock exchange	25
Government/state-owned enterprises	16
Others	8

Size of participating organisations

	% respondents
More than 10,000 employees	36
5,000 – 1,001 employees	21
500 – 101 employees	12
10,000 – 5,001 employees	11
1,000 – 501 employees	10
Up to 100 employees	8
Don't know	2

Participating industry groups

	% respondents
Financial services	20
Energy, utilities and mining	12
Professional services	9
Engineering and construction	7
Retail and consumer	7
Manufacturing	6
Technology	5
Insurance	4
Transportation and logistics	4
Communication	4
Other industries/business	4
Pharmaceuticals	3
Government / state-owned enterprises	3
Automotive	2
Chemicals	2
Entertainment and media	2
Hospitality and leisure	2
Aerospace and defence	1

Terminology

Accounting fraud

Financial statements and/or other documents are altered or presented in such a way that they do not reflect the true value or financial activities of the organisation. This can involve accounting manipulations, fraudulent borrowings/raising of finance, fraudulent application for credit and unauthorised transactions/rogue trading.

Asset misappropriation, including embezzlement/deception by employees

The theft of assets (including monetary assets/cash or supplies and equipment) by directors, others in fiduciary positions or an employee for their own benefit.

Bribery and corruption

The unlawful use of an official position to gain an advantage in contravention of duty. This can involve the promise of an economic benefit or other favour, the use of intimidation or blackmail. It can also refer to the acceptance of such inducements. Specific examples include kickbacks, extortion, gifts (with strings attached), facilitation payments, etc.

Competition law/anti-trust law

Law that promotes or maintains market competition by regulating anti-competitive and unfair business practices conduct by organisations. Examples may include price fixing, excessive, predatory or discriminatory pricing, unfair trading terms, and tying (i.e., stipulating that a buyer wishing to purchase one product must also purchase all or some of his requirements for a second product).

Cybercrime

Also known as computer crime is an economic offence committed using the computer and internet. Typical instances of cybercrime are the distribution of viruses, illegal downloads of media, phishing and pharming and theft of personal information such as bank account details. This excludes routine fraud whereby a computer has been used as a byproduct in order to create the fraud and only includes such economic crimes where computer, internet or use of electronic media and devices is the main element and not an incidental one.

Economic crime

The intentional use of deceit to deprive another of money, property or a legal right.

Espionage

Espionage is the act or practice of spying or of using spies to obtain secret information.

Financial loss

When estimating financial losses due to fraud, the participants should include both direct and indirect loss. The direct losses are the actual amount of fraud and the indirect losses would typically include the costs involved with investigation and remediation of the problem, penalties levied by the regulatory authorities, and litigation costs. This should exclude any amount estimated due to "loss of business opportunity".

Fraud risk assessment

Fraud risk assessments are used to ascertain whether an organisation has undertaken an exercise to specifically consider:

1. The fraud risks to which operations are exposed;
2. An assessment of the most threatening risks (i.e., Evaluate risks for significance and likelihood of occurrence);
3. Identification and evaluation of the controls (if any) that are in place to mitigate the key risks;
4. Assessment of the general anti-fraud programmes and controls in an organisation; and
5. Actions to remedy any gaps in the controls.

Human Resources fraud (recruitment and/or payroll fraud)

Fraud committed by members of the Human Resources department, including payroll fraud, ghost employees, pay-to-work, recruitment (i.e., hiring friends and/or relatives, hiring unqualified individuals, falsification of documents, etc.).

Incentive/pressure to perform

The individual has some financial problem that he/she is unable to solve through legitimate means so he/she begins to consider committing an illegal act as a way to solve the problem. The financial problem can be professional (e.g., job is in jeopardy) or personal (e.g., personal debt).

Insider trading

Insider trading refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, nonpublic information about the security. Insider trading violations may also include 'tipping' such information, securities trading by the person 'tipped', and securities trading by those who misappropriate such information.

IP infringement (including trademarks, patents, counterfeit products and services)

This includes the illegal copying and/or distribution of fake goods in breach of patent or copyright, and the creation of false currency notes and coins with the intention of passing with off as genuine.

Markets with a high level of corruption risk

While corruption risk levels can be subjective, for the purposes of this survey we suggest a territory with a Transparency International Corruption Perception Index ("CPI") score of 50 or less be considered a market with a high level of corruption risk. The link below the responses will direct you to the Transparency International list of territories and CPI scores.

Money laundering

Actions intended to legitimise the proceeds of crime by disguising their true origin.

Mortgage fraud

Mortgage fraud schemes employ some type of material misstatement, misrepresentation, or omission relating to a real estate transaction which is relied on by one or more parties to the transaction.

Opportunity or ability

The individual finds some way that he/she can use (abuse) his/her position of trust to solve the financial problem with a low perceived risk of getting caught.

Procurement fraud

Illegal conduct by which the offender gains an advantage, avoids an obligation or causes damage to his organisation. The offender might be an employee, owner, statutory board member, an official, a public figure or a vendor who was involved in the purchase of services, goods or assets for the affected organisation.

Rationalization

The individual finds a way to justify the crime to himself/herself in a way that makes it an acceptable or justifiable act.

Tax fraud

An illegal practice where an organisation or corporation intentionally avoids paying its true tax liability.

Contacts

Forensic services partners

John Wilkinson
Middle East Fraud and Forensics Leader
Dubai, UAE
Email: john.d.wilkinson@ae.pwc.com

Tania Fabiani
Middle East Fraud Risk and Integrity Leader
Abu Dhabi, UAE
Email: tania.fabiani@ae.pwc.com

Tareq Haddad
Middle East Investigations Leader
Riyadh, Saudi Arabia
Email: tareq.haddad@ae.pwc.com

Forensic services directors

Achraf El Zaim
Investigations, UAE
Email: achraf.elzaim@ae.pwc.com

James Tebbs
Head of Forensic Services, Qatar, Bahrain and Kuwait
Email: james.tebbs@qa.pwc.com

Courtenay Smith
Head of Corporate Intelligence, UAE
Email: courtenay.smith@ae.pwc.com

Matthew Fritzsche
Disputes, UAE
Email: matt.fritzsche@ae.pwc.com

Dean Gilbert
Head of Forensic Technology Services, UAE
Email: dean.gilbert@ae.pwc.com

Editorial team

Tareq Haddad
Email: tareq.haddad@ae.pwc.com

Anita D'Mello
Email: anita.dmello@ae.pwc.com

James Tebbs
Email: james.tebbs@qa.pwc.com

Tejasie Mendonca
Email: tejasie.mendonca@ae.pwc.com

Forensic Services

The PwC forensic services network is comprised of forensic accountants, economists, statisticians, former regulators and law enforcement, fraud examiners, and forensic technologists. We help organisations tackle the major financial and reputational risks associated with economic crime. We identify financial irregularities, analyse complex business issues, and mitigate the future risk of fraud.

www.pwc.com/me

To read our reports online scan the following QR codes on your smart phone or tablet.

Global Economic Crime Survey 2014

Middle East Economic Crime Survey 2014

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with close to 184,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

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

© 2014 PwC. All rights reserved. PwC refer to the PwC network and/or one or more of its member firms, each of which is a separate legal entity.Please see www.pwc.com/structure for further details.

CDC/625/(2/2014)