www.pwc.com/crimesurvey

Economic Crime in the Arab World

Global Economic Crime Survey

Middle East report

January 2012

pwc

With 3,877 responses from senior executives in 78 countries world-wide, this is the most comprehensive global survey of economic crime available to businesses

Contents

Foreword

Economic crime is a truly global phenomenon. In our region, the perception of a high level of corruption has caused great dissatisfaction amongst some of the populace of the Arab World

We are pleased to present the results from the PwC Global Economic Crime Survey 2011 with special focus on the Middle East. With 3,877 responses from senior executives in 78 countries world-wide, this is the most comprehensive global survey of economic crime available to businesses. For the Middle East survey, we received 126 responses from representatives in organisations in Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Oman, Qatar, Saudi Arabia, United Arab Emirates and the West Bank Region.

Our survey assesses the levels and most common types of economic crime, existing frameworks to prevent and detect fraud, the profile of fraudsters and the expectations of respondents as to whether economic crime will increase in the future. In this report, we compare the responses received from the Middle East to the global responses.

Governments, as well as commercial organisations, are realising the increasing importance of fighting fraud and corruption. Some governments have proactively taken steps to fight corruption. For example, the Abu Dhabi Accountability Authority (ADAA), formed in 2008, in the United Arab Emirates has (as part of its mandate to provide assurance at a public entity level) implemented an anti-fraud programme for Abu Dhabi's public entities. As part of this anti-fraud programme, ADAA has encouraged and supported organisations to conduct fraud risk assessments, adopt and implement anti-fraud policies and launch whistle-blowing mechanisms. In 2009, the Kurdistan Regional Government announced a comprehensive anti-corruption and transparency strategy, in 2010, established the Office of Governance and Integrity, and, in 2011, issued a code of conduct for public servants and mandated financial disclosure by certain government officials. Also, the Kingdom of Saudi Arabia has established the National Anti-Corruption Commission in 2011.

Economic crime is a truly global phenomenon. In our region, the perception of a high level of corruption has caused great dissatisfaction amongst some of the populace of the Arab World. The people have sent strong messages that they expect their governments and communities to fight corruption. Many governments in the Middle East have taken steps to proactively fight corruption but robust anti-corruption frameworks can only be built through sustained effort over time.

Our survey shows that economic crime continues to be a persistent facet threat of business life in the Middle East. Of the respondents in the Middle East, 28% say that they have experienced economic crime in the last 12 months, However, it is possible that more organisations in the Middle East suffer from economic crime but do not have the robust detection mechanisms that would allow accurate reporting. Alarmingly, our survey showed that Middle East respondents believe they are 50% more likely (compared with global figures) to be affected by an incidence of corruption over the next 12 months.

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. We hope that the information contained in this report will assist you and your organisations in fighting economic crime.

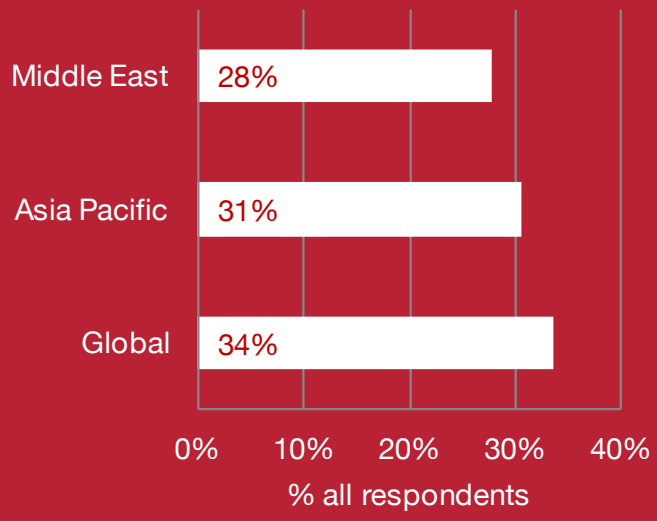
Tareq Haddad
Partner – Middle East Forensic Services

Executive summary

What is the level of economic crime in the Middle East and in what direction is it heading?

Our survey shows that 28% of respondents in the Middle East experienced economic crime during the last 12 months compared to the global average of 34%.

Figure 1: Experience of economic crime

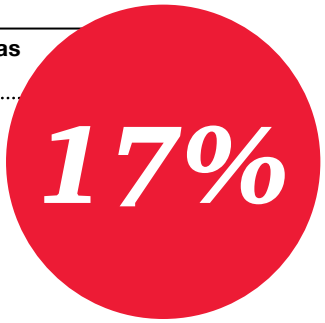


Respondents in the Middle East also indicated that some types of economic crime occur at a higher frequency, including:

- asset misappropriation (71%);
- bribery and corruption (43%);
- cybercrime (40%); and
- accounting fraud (31%).

However, it is worrying to note that almost 39% of the Middle East respondents expect that their organisations will experience bribery and corruption in the next 12 months compared to the global average of 23%. This clearly indicates that respondents expect to see more economic crime in the Middle East.

17% of Economic crime was detected by accident



How do organisations detect economic crime?

Our survey showed that Middle East organisations detect fraud through corporate controls less frequently than the global average. Alarmingly, 17% of fraud incidents in the Middle East were detected by accident compared to a global average of 8%. These results are perhaps an indicator that fraud detection measures could be better integrated within corporate controls in Middle East organisations. This could be achieved, for example, by ensuring that internal audit staff are adequately trained in fraud detection techniques.

In our experience, organisations that have developed fraud detection mechanisms and implemented fraud awareness programmes for their employees are better at detecting fraud.

Who's committing this fraud?

When assessing whether perpetrators of economic crime were internal or external to their organisations, 69% of respondents in the Middle East indicated that economic crimes suffered by their organisations were internally perpetrated, which is higher than the global average of 56%. The survey also revealed that a 'typical' internal fraudster is male, in middle management, aged 31 to 40 years, holding a graduate degree and that many (42%) have been with the organisation between 3 to 5 years.

What is the cost of fraud and what is the collateral damage?

Of the respondents whose organisations suffered from economic crime in the last 12 months, almost half indicated that the total losses suffered by their organisations were between USD 100,001 and USD 5 million. A further 14% of these respondents indicated that their organisation suffered losses higher than USD 5 million.

The collateral costs associated with economic crime are equally important when trying to assess the impacts of fraud. Our respondents indicated that the most adverse collateral impacts related to employee morale, reputation and brand of the organisation and business relations. More than 1 in 5 respondents indicated that economic crime incidents had a significant effect on all three. It is also interesting to note that economic crime has a more significant effect on share prices in the Middle East when compared to the global average.

Cybercrime: a growing threat in the Middle East

Interestingly, cybercrime incidents occur at a higher rate in the Middle East than globally. 40% of Middle East respondents stated that their organisation had been a victim of cybercrime whilst the global average lies at 23%. The perception of about 45% of the respondents in the Middle East is that cybercrime has increased in the last 12 months and more than half of the respondents felt that their organisations were exposed to the risk of cybercrime from within and from outside their country of operations.

The highlights

Economic crime in the Middle East:

- 28% of Middle East respondents experienced economic crime in the last 12 months
- Asset misappropriation, bribery and corruption, cybercrime and accounting fraud were the most common types of fraud reported
- Fraud is most commonly detected by accident
- Almost 2 in 5 respondents in the Middle East reported that their organisations have not performed a fraud risk assessment in the last 12 months
- 69% of respondents indicated that the most serious fraud in their organisations was perpetrated by an insider
- Almost half of Middle East respondents who reported fraud suffered losses between USD 100,001 and USD 5 million and 14% indicated that they suffered a loss of more than USD 5 million
- 25% of Middle East respondents indicated that their organisations decided not to enter a new venture or market in the last 12 months due to corruption risk

Cybercrime in the Middle East:

- Of those respondents who reported economic crime in the Middle East 40% experienced cybercrime
- Just over half of respondents feel that their organisation's information technology departments pose the highest cybercrime risk
- Over 35% of respondents in the Middle East feel their organisations have insufficient in-house capabilities to prevent, detect and investigate cybercrime
- Respondents in the Middle East are seriously concerned by the effects cybercrime has on their reputation, theft of their intellectual property and the loss or theft of personal information

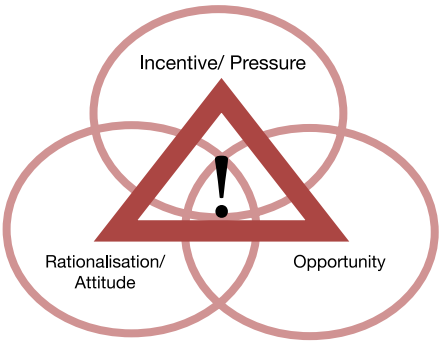
The future trends of fraud in the Middle East:

- Respondents in the Middle East expect their organisations to experience an increase in economic crime in the region, with almost 39% expecting incidents of bribery and corruption in the next 12 months
- More respondents in the Middle East expect to face incidents of accounting fraud and money laundering than the global average

28% of respondents said that their organisations have experienced fraud in the last 12 months

28%

Economic crime in the Middle East



The fraud triangle

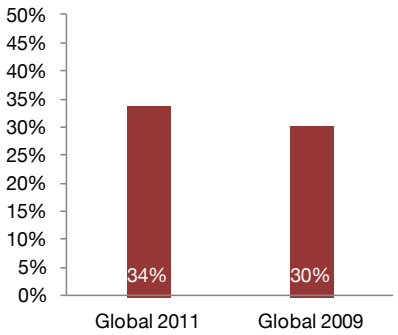
The fraud triangle identifies three conditions that are commonly found when fraud occurs. First, the perpetrator experiences some form of incentive or pressure. Second, there must be an opportunity to commit fraud. Third, the perpetrators must be able to rationalise or justify their actions. It is useful to keep the fraud triangle in mind when considering the results of our survey and, in particular, when seeking to understand how and why fraud has occurred.

Our survey shows that economic crime is on the rise globally, with incidents of fraud rising from 30% to 34%. Since this is the first Middle East survey, we do not have 2009 comparative data for the Middle East.

Unsurprisingly, asset misappropriation was the most common type of economic crime to occur globally. Of the Middle East respondents whose organisations reported fraud, 71% experienced asset misappropriation during the last 12 months.

Differences between the global and Middle East results emerge in the prevalence of bribery and corruption, cybercrime, accounting fraud and money laundering. All are types of economic crime that are expected to occur at a higher rate in the Middle East when compared to the global average. For example, bribery and corruption was present in 43% of incidents of economic crime in the Middle East, which is almost double the global rate of 24%. This may explain why 25% of participants noted that their organisation did not enter a new venture or market in the last 12 months due to corruption risks. It is also unsurprising when one considers that, in Transparency International's[1] 2011 Corruption Perceptions Index[2], the majority of Middle Eastern countries scored lower than 5 on a scale of 1 to 10

Figure 2: Organisations that have experienced economic crime in the last twelve months



[1] "Transparency International is a global network including more than 90 locally established national chapters and chapters-in-formation. These bodies fight corruption in the national arena in a number of ways" –www.transparency.org

[2] With 1 being perceived to be the most corrupt and 10 perceived to be the least corrupt, the Corruption Perceptions Index provides a measure of the perceived corruption level of a country.

43%

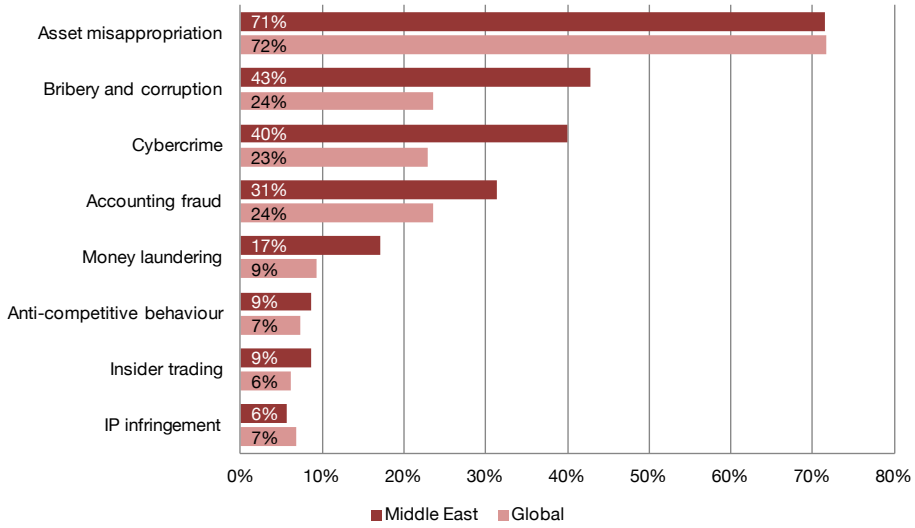
43% of Middle East respondents whose organisations experienced economic crime reported that the crime included elements of bribery and corruption

Money laundering poses a serious risk to organisations in the Middle East. Of all the economic crimes reported by Middle East respondents, 17% involved money laundering, compared to the global average of 9%. Regulators will need to be vigilant to ensure that the risk of money laundering is contained and reduced to ensure minimal effect on an already fragile post-financial crisis economy.

Accounting fraud is another type of economic crime that appears to have been more prevalent in the Middle East than globally over the last 12 months. 31% of respondents whose organisations reported economic crime in the Middle East had suffered accounting fraud in the last 12 months. This is higher than the global average of 24%.

Finally, the survey notes that cybercrime was experienced by 40% of respondents whose organisations had experienced economic crime in the last 12 months.

Figure 3: Types of economic crime suffered in the last 12 months*



**Note: Respondents that reported experiencing some form of economic crime in the last 12 months were asked to identify all types of economic crime they had suffered - hence the total is greater than 100%.*

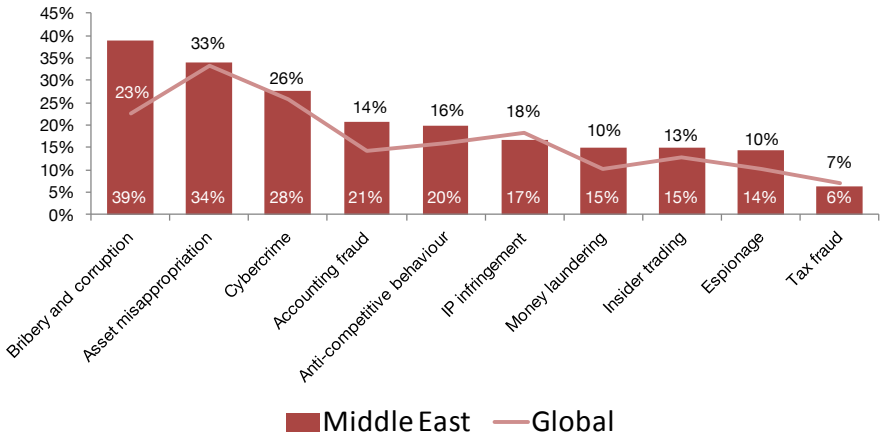
More than 27% of Middle East respondents expect their organisations to be exposed to asset misappropriation, bribery and corruption, or cybercrime in the next 12 months

Almost 2 in 5 Middle East respondents expect their organisations to experience bribery and corruption in the next 12 months

2 in 5

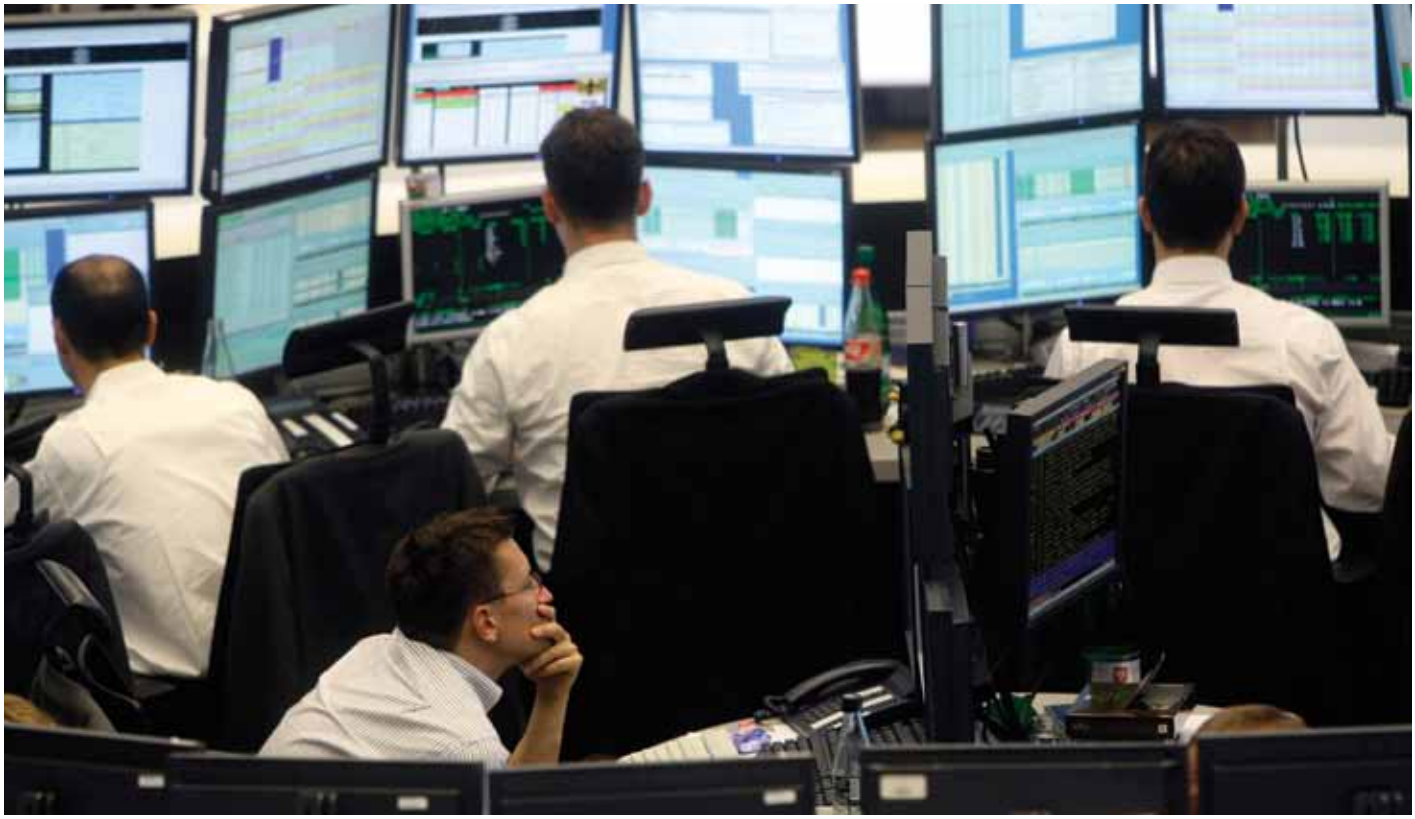
Respondents see more fraud ahead

Figure 4: Types of fraud: Future expectations



It is worrying to note that almost 39% of respondents in the Middle East think their organisations are likely to face incidents of bribery and corruption in the next 12 months. This rate is more than once and a half times the global average of 23%. A significant finding is that respondents expect their organisations to experience bribery and corruption in the next 12 months at a higher rate than those that have actually experienced incidents of bribery and corruption in the last 12 months.

Similarly, the level of accounting fraud, anti-competitive behaviour, money-laundering and espionage expected to occur in the Middle East over the next 12 months is higher than the global average.



What are organisations in the Middle East doing to detect and mitigate fraud?

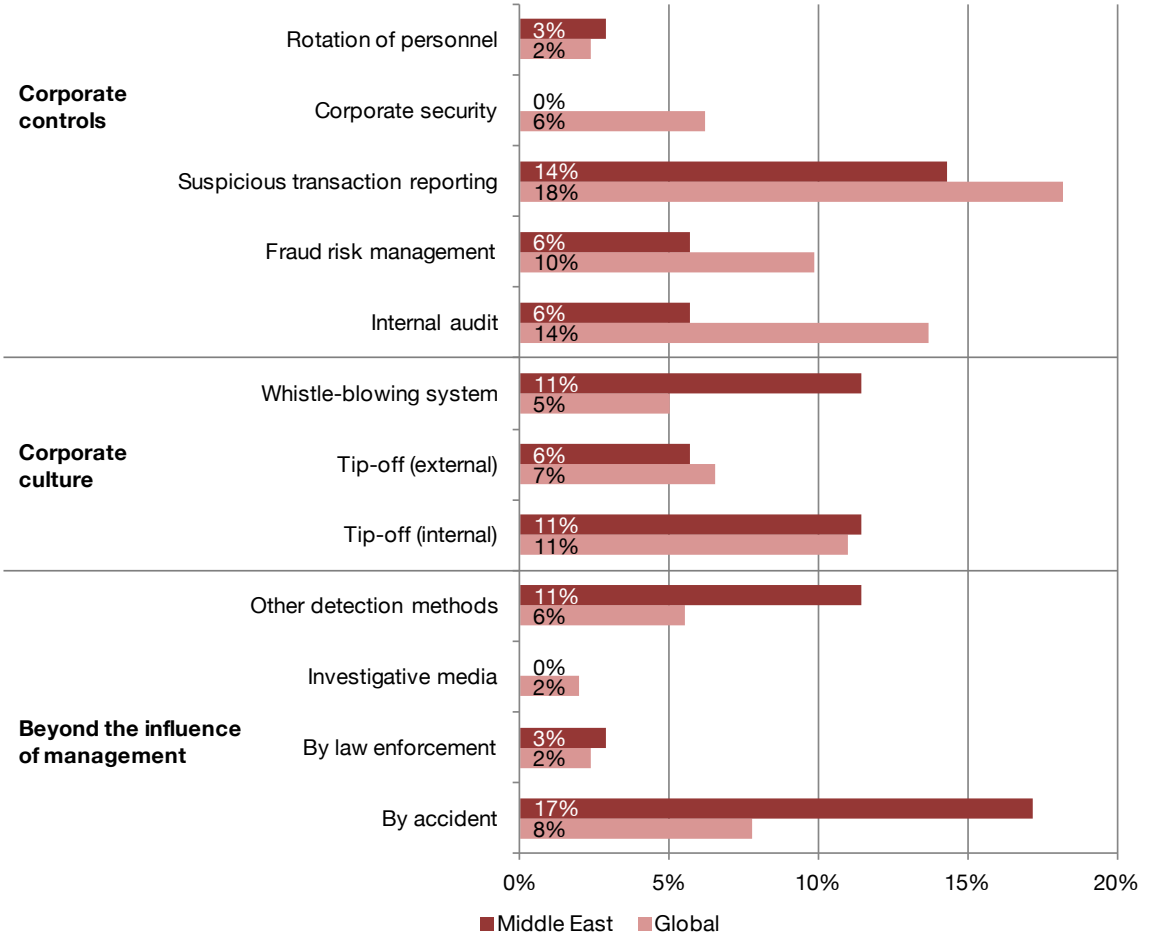
There is no sure way of completely eliminating the risk of fraud. Organisations can help to mitigate fraud risk by taking a proactive approach to ensuring that fraud prevention and detection mechanisms are effective in addressing the significant risks of fraud.

Figure 5 shows that Middle East organisations detected fraud through corporate controls less frequently than the global average. Alarmingly, 17% of fraud incidents in the Middle East were detected by accident compared to a global average of 8%. Another cause for concern is that only 6% of incidents of economic crime were detected through routine internal audits, suggesting that internal audits are not adequately geared towards detecting fraud.

These results are perhaps an indicator that fraud detection measures could be better integrated within corporate controls in Middle East organisations, for example, by ensuring that internal audit staff are adequately trained in fraud detection techniques. It is worth noting, however, that 17% of incidents were identified through tip-offs (internal and external) and 11% were detected through a formal whistle-blowing mechanism.

A fraud risk assessment is one of the main components for an effective fraud risk management programme.

Figure 5: How did organisations detect economic crime?

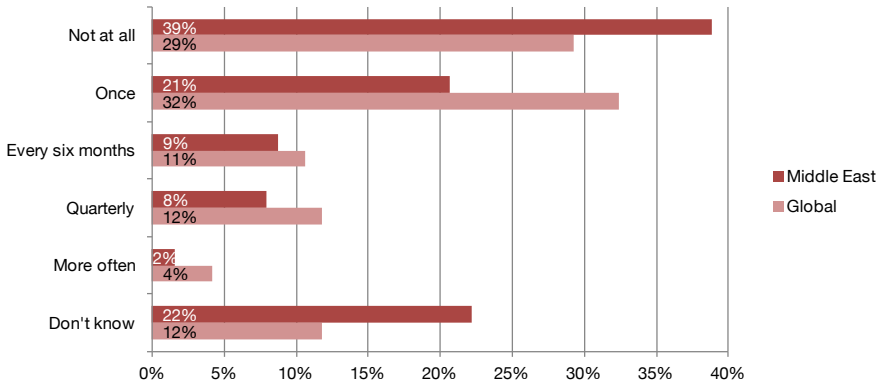


69% of respondents indicated that fraud suffered by their organisations was internally perpetrated

When asked whether their organisations had performed a fraud risk assessment in the last 12 months, 39% of our respondents stated that an assessment had not been performed and 22% were unaware of whether or not an assessment had taken place. As shown in figure 6, fraud risk assessments are less frequently performed in the Middle East than globally.

Respondents in the Middle East that indicated that their organisation had not performed a fraud risk assessment in the last 12 months were asked the underlying reason for not conducting such an assessment: 35% responded that it was due to a perceived lack of value while 31% indicated they were uncertain as to what a fraud risk assessment entails.

Figure 6: How often does your organisation perform a fraud risk assessment?



Who are the perpetrators?

We collected information about the perpetrators of economic crimes in order to better understand the characteristics of those who committed fraud in the last 12 months.

We asked respondents whether perpetrators of economic crimes were internal or external to their organisations. Worryingly, a high proportion of respondents in the Middle East (69%) indicated that economic crimes suffered by their organisations were internally perpetrated. This is higher than the global average of 56%.

Respondents in the Middle East who indicated that they had experienced economic crime perpetrated by an internal party reported that 42% of the incidents were committed by middle management. This strong correlation between perpetrators of economic crime and position within the victim organisation can be explained by their knowledge of the organisations' systems and how to circumvent controls in order to commit economic crimes.

Figure 7: Perpetrators

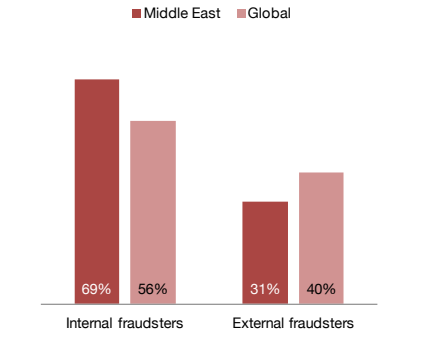


Figure 8: The profile of a perpetrator

92% are male

63% hold a graduate degree

54% are 31 to 40 years old

42% have a tenure of 3 to 5 years in the organisation

According to our survey, the 'typical' internal fraudster is a middle management male employee, aged 31 to 40 years, who holds a graduate degree and many (42%) have been with the organisation between 3 to 5 years.

What actions are taken against the perpetrators?

38% of respondents indicated that their organisations notified law enforcement agencies and took civil action against perpetrators, which indicates that organisations in the Middle East seem to be willing to prosecute perpetrators when fraud is detected. Furthermore, 21% of organisations in the Middle East notified the relevant regulatory authority when they suffered an economic crime, higher than the global average of 17%.

How does economic crime impact organisations in the Middle East?

Measuring the cost of economic crime is an extremely challenging endeavour. The inherently hidden nature of economic crime means that we are able to only measure the amounts that are uncovered or reported. This is why any measurement will be an estimate at best.

In its 2010 Report to the Nations[3], the Association of Certified Fraud Examiners[4] (ACFE) report the results of a survey that indicated median average losses of 5% of organisations' annual revenues to occupational fraud and abuse. The ACFE Report applied this percentage to the 2009 estimated Gross World Product of USD 58.07 trillion, which resulted in a projected total global fraud loss of more than USD 2.9 trillion.

Figure 9: Actions taken against fraud perpetrators

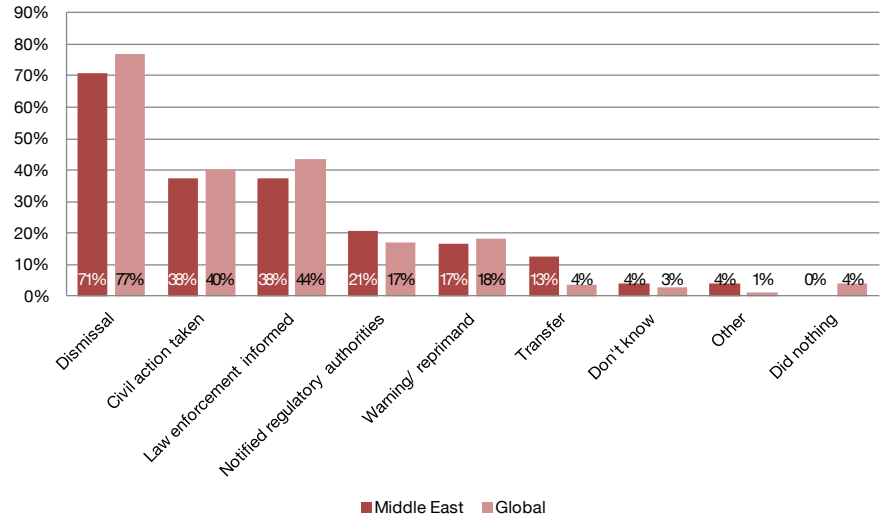
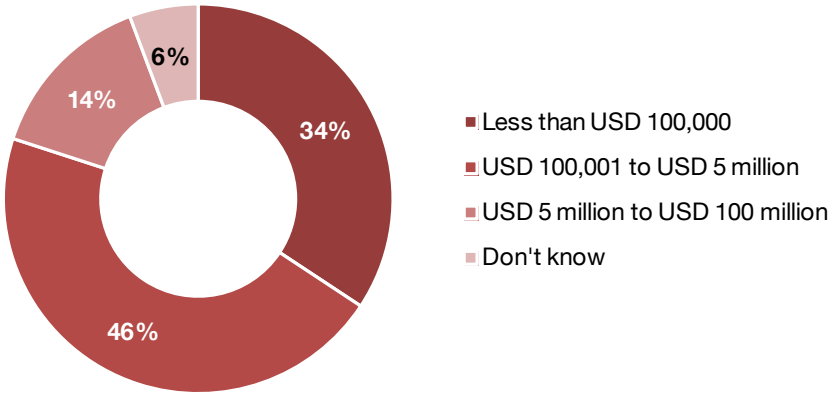


Figure 10: Financial loss from incidents of economic crime



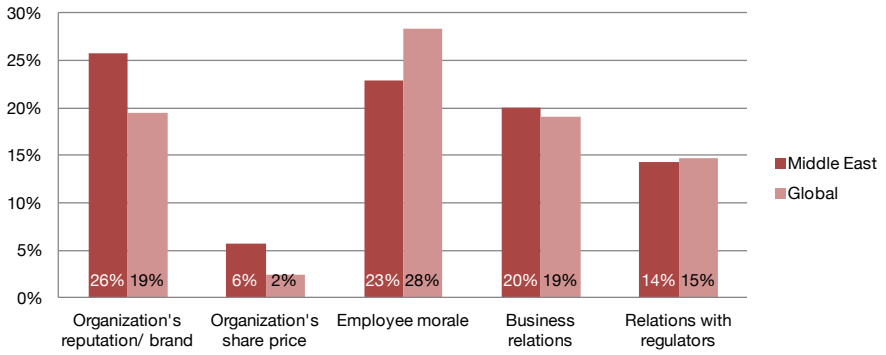
[3] Report to the Nations on Occupational Fraud and Abuse, 2010 Global Fraud Study, Association of Certified Fraud Examiners

[4] "The ACFE is the world's largest anti-fraud organisation and premier provider of anti-fraud training and education." - www.acfe.com

Almost 1 in 6 victims of fraud lost more than $ 5 million

Almost 63% of victim respondents' organisations reported experiencing between 1 to 10 incidents of economic crime in the last 12 months with over 45% of victim respondents stating costs between USD 100,001 and USD 5 million. Victim participants also reported that about 1 out of every 6 incidents (14%) had resulted in a financial loss of more than USD 5 million as compared to the global average of 1 in 10 incidents.

Figure 11: Significant effects of economic crime



The effects of economic crime extend to include collateral consequences such as damage to the brand, reputation and employee morale. From a collateral perspective, 26% of Middle East respondents whose organisations experienced economic crime in the last 12 months noted that incidents of economic crime had a significantly adverse effect on their organisation's reputation and brand, while 23% noted a significantly adverse effect on employee morale and 20% of the respondents noted a significantly adverse effect on business relations. Additionally, 6% of respondents noted that economic crime had an effect on their organisations' share price, which is significantly higher than the global average of 2%. All of these collateral impacts could have serious financial consequences, for example, damage to the brand or reputation of a company could result in reduced sales.

Cybercrime in the Middle East

45%

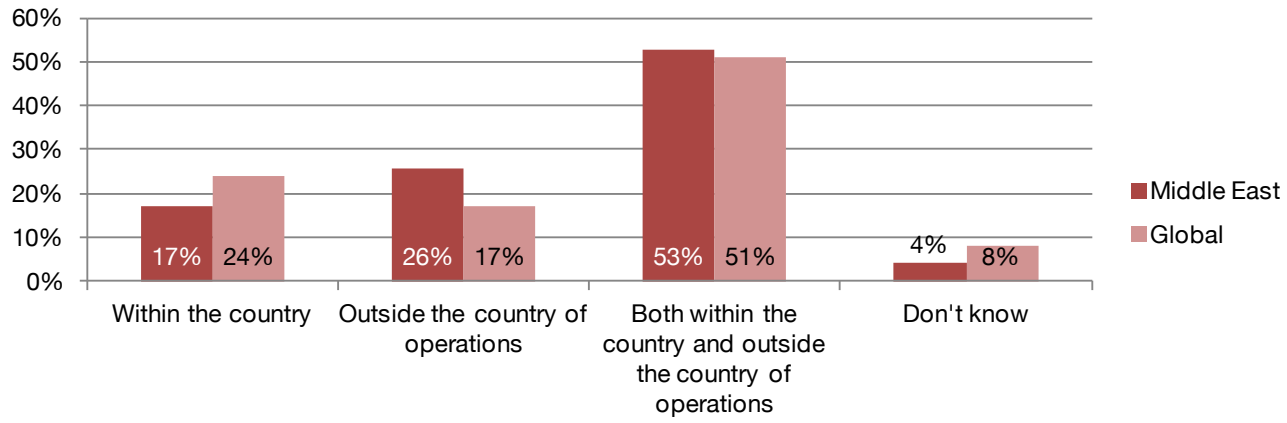
of respondents in the Middle East felt that they have adequate in-house capabilities to detect and prevent cybercrime

For the purposes of our survey, we defined cybercrime as an economic crime committed using computers and the internet. It includes distributing viruses, illegally downloading files, phishing and pharming, and stealing personal information like bank account details. It's only a cybercrime if a computer, or computers, and the internet play a central role in the crime, and not an incidental one.

What does cybercrime in the Middle East look like?

It is alarming to note that 40% of respondents in the Middle East, who had been victim of economic crimes in the last 12 months, stated that they experienced a form of cybercrime. This percentage is higher than the global average of 23%. As such, it is not surprising that 45% of Middle East respondents perceive that the risk of cybercrime has increased during the last 12 months.

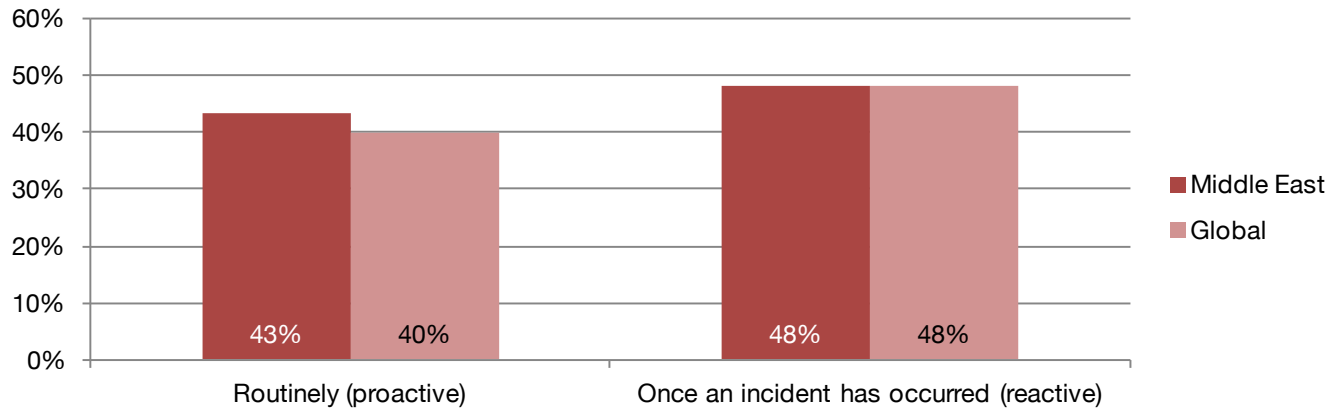
Figure 12: Cybercrime risk by boundaries



Regarding the perception of cybercrime threats, 26% of respondents in the Middle East felt that the threat of cybercrime was external to their country of operations, which is higher than the global average, while 53% of the respondents felt that their organisations were exposed to cybercrime from both within and outside the country of operations.

In addition to being asked about how their organisations deal with cybercrime, respondents were asked about the timing of hiring external experts. 48% of respondents in the Middle East indicated that their organisation consults with an external expert when a cybercrime incident occurs while 43% of the same respondents indicated that they consult with external experts proactively and on a routine basis.

Figure 13: When are external experts engaged?



How does cybercrime affect organisations?

The survey showed that organisations in the Middle East worry most about reputational damage, intellectual property theft and loss or theft of personal information (including customer information) as a consequence of cybercrime. Interestingly, respondents in the Middle East were least concerned with the cost of investigation and damage control.

Is cybercrime combated adequately?

While many organisations are aware of the threat of cybercrime, only 45% of respondents in the Middle East, compared to 60% of respondents globally, felt that they have adequate in-house capabilities to detect and prevent cybercrime. 36% felt that they do not have adequate in-house capabilities to detect and mitigate cybercrime, compared to only 25% of global respondents..

The majority of the Middle East respondents reported that they did not have or did not know if they had an adequate media and public relations plan in place to deal with the occurrence of cybercrime.

Furthermore, reactive measures to cybercrime are still not as advanced in the Middle East as they are on a global level, with 46% of respondents in the Middle East indicating that they have adequate emergency shutdown procedures, as opposed to 54% of global respondents.

Figure 14: Cybercrime - what keeps organisations awake?

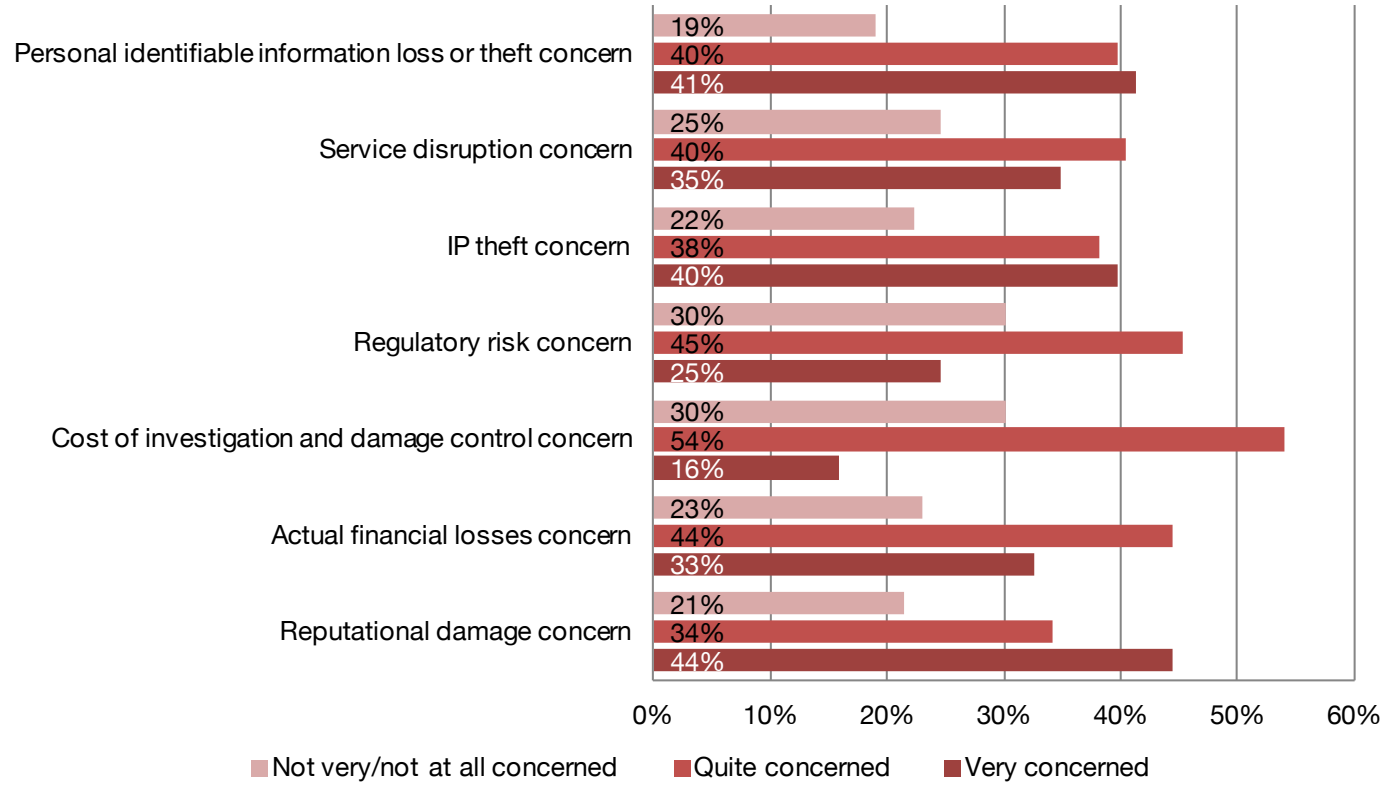
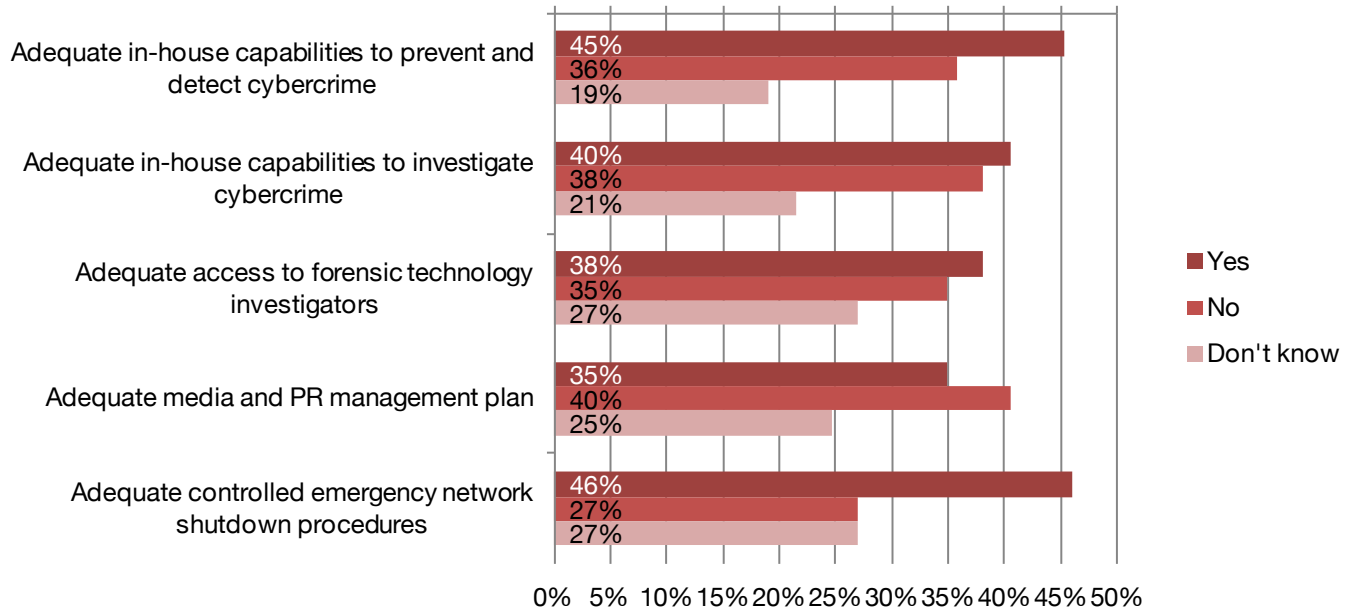


Figure 15: Adequate measures for prevention and detection



Methodology and acknowledgements

We carried out our sixth Global Economic Crime Survey between June 2011 and November 2011.

About the survey

The 2011 Global Economic Crime Survey: Middle East Report was completed by 126 respondents. Of the total number of respondents, 37% were senior executives in their respective organisations, 42% were C-Suite executives, 26% represented listed companies and 42% represented organisations with more than 1,000 employees.

We conducted a survey of executives in organisations in the Middle East and globally. The findings in this survey come from executives reporting their experiences of economic crimes in their organisations. We obtained information from them on the different types of economic crime, their impact on the organisation (both the financial loss and any collateral damage), the perpetrators of these crimes, what action the organisation took and how they responded to the crime.

Figure 16: Job titles of participants

	% respondents
Manager	20%
Chief Financial Officer/ Treasurer/ Comptroller	17%
Senior Vice President/ Vice President/ Director	15%
Other C-level Executive	13%
Head of Department	13%
Head of Business Unit	9%
Chief Executive Officer/ President/ Managing Director	7%
Chief Operating Officer	3%
Chief Information Officer/ Technology Director/ Chief Security Officer	2%
Board member	1%

Figure 17: Function (main responsibility) of participants in the organisations

	% respondents
Finance	23%
Audit	18%
Executive management	14%
Compliance	9%
Advisory/ Consultancy	7%
Legal	5%
Risk management	5%
Information technology	4%
Operations and production	4%
Other	3%
Customer service	2%
Research and Development	2%
Security	2%
Human resources	1%
Marketing and sales	1%
Procurement	0%
Tax	0%

Figure 18: Participating organisation types

	% respondents
Private	48%
Listed on a stock exchange	26%
Government/ state-owned enterprises	25%
Cooperative/ non- profit organisations	1%

Figure 19: Size of participating organisations

	% respondents
Up to 200 employees	35%
201 to 1,000 employees	20%
1,001 to 5,000 employees	26%
More than 5,000 employees	16%
Don't know	3%

Figure 20: Participating industry groups

	% respondents
Financial services	24%
Energy, utilities and mining	9%
Engineering and construction	9%
Manufacturing	9%
Government / state-owned enterprises	8%
Professional services	7%
Hospitality and leisure	6%
Transportation and logistics	5%
Other industries/ business	4%
Retail and consumer	3%
Aerospace and defence	2%
Entertainment and media	2%
Technology	2%
Property	2%
Automotive	1%
Chemicals	1%
Communication	1%
Insurance	1%
Pharmaceuticals and life sciences	1%
Education	1%
Health and care	1%
Food related	1%

Terminology

Due to the diverse descriptions of individual types of economic crime in countries' legal statutes, we developed the following categories for the purpose of this survey. These descriptions were defined in the web survey to assist respondents in completing the survey.

Economic crime or fraud

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

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.

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.

Corruption and bribery (including racketeering and extortion)

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.

Money laundering

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

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 off as genuine.

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, non-public 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.

Espionage

Espionage is the act or practice of spying or of using spies to obtain secret information or using technology to act on your behalf as spies.

Financial performance

This can be defined as measuring the results of an organisation's policies and operations in monetary terms. These results are reflected in return on investment, return on assets and value added; typically, in the private sector, returns will be measured in terms of revenue; in the government/ state-owned enterprises, returns will be measured in terms of service delivery.

Fraud risk assessment

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

- The fraud risks to which an organisation is exposed;
- An assessment of the significant risks (i.e. evaluate risks for significance and likelihood of occurrence);
- Identification and evaluation of the controls (if any) that are in place to mitigate the key risks;
- Assessment of the general anti-fraud programmes and controls in an organisation; and
- Actions to remedy any gaps in the controls.

Fraud triangle

Fraud triangle describes the interconnected conditions that act as harbingers to fraud: opportunity to commit fraud, incentive (or pressure) to commit fraud, and the ability of the perpetrator to rationalise the act.

Senior executive/ C-Suite

The senior executive (for example the CEO, Managing Director or Executive Director) is the main decision maker in the organisation.

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 by product 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.

Anti-competitive behaviour

Includes practices that prevent or reduce competition in a market such as cartel behaviour involving collusion with competitors (for example, price fixing, bid rigging or market sharing) and abusing a dominant position.

Financial losses

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, litigation costs, and reputational damage. This should exclude any amount estimated due to "loss of business opportunity".

Cybercrime incident response mechanism

This would typically include in-house technical capabilities to prevent, detect and investigate cybercrime, access to forensic technology investigators, media and public relations management plan, controlled emergency network shut down procedures, etc.

About PwC Forensic Services

The Forensic Services group of PricewaterhouseCoopers' global network of firms plays a lead role in addressing the life cycle of fraud other avoidable losses, providing reactive investigative services proactive remedial and compliance to clients in the public and private sector. The Middle East Forensic Services team has the ability to conduct its work and report both in the English and Arabic languages.

The PwC global 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.

Contacts

Forensic Services

Tareq Haddad
Partner, Middle East
Forensic Services
+971 (0) 50 189 6066
tareq.haddad@ae.pwc.com

Achraf ElZaim
Director, Middle East
Forensic Services
+971 (0) 56 682 0532
achraf.elzaim@ae.pwc.com

Bissan Al-Shami
Senior Manager, Middle East
Forensic Services
+971 (0) 56 682 0699
bissan.al-shami@ae.pwc.com

Maleeha Ali
Senior Manager, Middle East
Forensic Services
+971 (0) 56 682 0661
maleeha.ali@ae.pwc.com

Matt Fritzsche
Senior Manager, Middle East
Forensic Services
+971 (0) 56 682 0660
matt.fritzsche@ae.pwc.com

Ruth Button
Manager, Middle East
Forensic Services
+971 (0) 50 900 7664
ruth.button@ae.pwc.com

Zayd Sukhun
Senior Consultant, Middle
East Forensic Services
+971 (0) 4 304 3372
zayd.sukhun@ae.pwc.com

Fraud Risk Assurance

Tania Fabiani
Middle East Leader and
Partner, Fraud Integrity
Compliance Risk Assurance
(FICRA)
+971 (0) 50 642 4483
tania.fabiani@ae.pwc.com

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 169,000 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 2,500 people. (www.pwc.com/middle-east)

Designed by CDC 194 (1/2012)

www.pwc.com/crimesurvey