2020

Harnessing technology to combat fraud

PwC Middle East Economic Crime and Fraud Survey

pwc

www.pwc.com/me/fraudsurvey

Rising crime highlights the need for new capabilities

Our 2020 Economic Crime and Fraud Survey indicates that organisations across the Middle East remain vulnerable to traditional economic crimes that have afflicted the region for centuries. Bribery, procurement fraud and other forms of corruption are still prevalent. At the same time, Middle East organisations, like their global competitors, are the subject of increasingly sophisticated forms of economic crimes, including from cyber-threat actors that possess the technology and expertise to infiltrate corporate databases from anywhere in the world. Organisations operating in the region must proactively arm themselves in order to mitigate the potential financial and reputational impact of economic crime.

As fraud continues to emerge as a greater and more costly threat than ever, the message from our 2020 survey is clear, organisations across the Middle East must act quickly by harnessing emerging technologies and strengthening their anti-fraud capabilities to ensure they are ready and equipped to tackle familiar and unfamiliar threats, whenever they appear. As previously identified in our 2018 survey, the importance of knowing your business thoroughly and investing wisely in people should not be underestimated in mitigating the risk of fraud and other forms of economic crime.

46%

of **Middle East** respondents said that their organisation has experienced fraud, corruption or some other form of economic crime **within the last two years**

Almost the same proportion as the **global average** of

47%

However, this represents a **sharp increase** for the region **since 2018**, when the figure was

34%

The optimistic view is that Middle East organisations are becoming more effective at identifying and assessing the damage caused by fraud. However, a more detailed look at the regional results indicate that organisations are still not tackling fraud and economic crime in a comprehensive and consistent way.

21%

of respondents said that financially they don't know how much money was lost to fraud incidents in all its forms in the past two years

More than three times the global survey average of

7%

In line with the global survey, the results from our Middle East respondents also suggest that too many organisations are falling short in their duty to report known cases of fraud to corporate boards, despite a growing focus on integrity and compliance throughout the region.

The nature of the threat is changing. While the region continues to experience traditional frauds such as bribery, an increasing number of crimes are committed by perpetrators using sophisticated technology to breach inadequate security firewalls. Like their global peers, Middle East organisations are aware of the threat from cyber-attacks and the need to strengthen their capabilities to defend against it, yet so far they are not taking sufficient remedial action.

Against this background, the survey results from our sample of 82 executives with senior responsibility or direct oversight of anti-fraud systems and policies, suggest that Middle East organisations need to take the same anti-fraud actions as their global peers, paying particular attention to their technological measures and compliance procedures. There are three key steps to consider:

01 Assess readiness

Is your organisation assessing potential frauds efficiently?

02 Deploy effective measures

Do compliance and anti-fraud controls and systems provide adequate security, or are there gaps in the defences?

03 Harness emerging technologies

Is your organisation sufficiently enabled with the latest 'smart', digitalised compliance and anti-fraud systems?

Assess readiness

Fraud and economic crime in the Middle East is taking increasingly diverse forms, in line with the global trend. Identifying the different kinds of threats is the first step to understanding an organisation's particular vulnerabilities and ensuring that it has adequate anti-fraud defences.

In the region, traditional fraud types continue to feature prominently, compared with the global survey average. **Procurement fraud**, which may include the practice of favouring known associates with vendor and supplier contracts, remains a significant and growing problem. In 2018, 22% of Middle East respondents said their organisation had suffered procurement fraud. This year, the proportion has risen to 42%, more than double the global survey average of 19%.

Customer fraud is also a growing problem for Middle East organisations, with 47% of respondents reporting an incident during the past two years, up from 36% in 2018. Meanwhile, **bribery and corruption** remain familiar challenges across the region, although the results do not present an entirely consistent picture. On the one hand, 18% of respondents said their organisation has been asked to pay a bribe, lower than the global average of 29%. On the other hand, 45% of respondents in the region said they uncovered cases of bribery and corruption in the past two years, 15% higher than the worldwide proportion.

Too many businesses in the region are also challenged to meet compliance obligations by reporting known cases of fraud to corporate boards. Only 26% of the Middle East respondents said they informed their board about incidents of fraud or other economic crimes in the last two years, a significantly lower proportion than the global average of 35%. This was despite 76% of Middle East respondents who said they launched an investigation after a fraud or economic crime had been committed, compared with 56% globally.

Respondents who said their organisation experienced procurement fraud in the past two years

42% Middle East 2020 | **22%** Middle East 2018 | **19%** Global 2020

Respondents who said their organisation experienced customer fraud in the past two years

47% Middle East 2020 | **36%** Middle East 2018

Respondents who said their organisation uncovered cases of bribery and corruption in the past two years

45% Middle East 2020 | **30%** Global 2020

Respondents who said their organisation was asked to pay a bribe in the past two years

18% Middle East 2020 | **29%** Global 2020

Respondents who said they informed their board about fraud or economic crime incidents in the past two years

26% Middle East 2020 | **35%** Global 2020

Respondents who said they launched an investigation after a fraud or economic crime was committed in the past two years

76% Middle East 2020 | **56%** Global 2020

21% of the Middle East respondents identify procurement fraud as one of the **most disruptive** types of economic crime to hit their organisation compared to **6%** globally.

Deploy effective measures

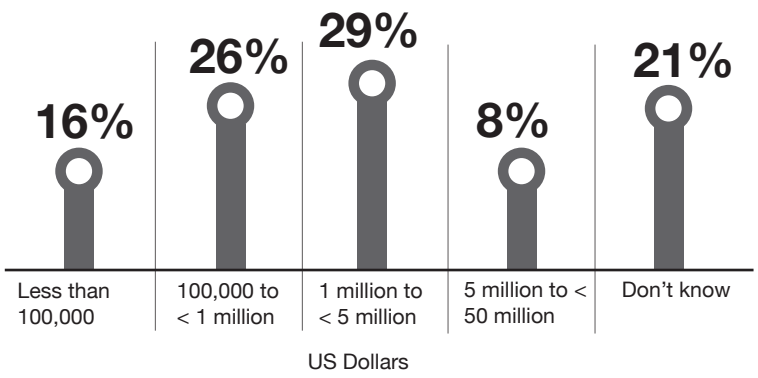
A lack of information at boardroom level helps to explain why many Middle East organisations struggle to measure the scale of the damage to their organisations inflicted by fraud, corruption and other economic crime. 21% of Middle East respondents said they do not know how much money has been lost to fraud in all its forms during the past two years, more than three times the global survey average of 7%.

These figures suggest a gap between the good intentions of Middle East organisations to prevent and detect fraud and other economic crimes, and their ability to improve their performance in this area. In general terms, Middle East organisations compare well with the overall survey regarding their anti-fraud commitments: 63% of regional respondents said that following an incident they have implemented or enhanced internal controls, compared with 44% globally. A further 61% reported that they have implemented or enhanced anti-fraud policies and procedures; the equivalent worldwide figure is 39%.

Middle East organisations also score well relative to the overall survey regarding personnel issues arising from fraud, corruption and economic crimes. 42% of Middle East respondents said they have disciplined or let go of staff as a result of an incident, slightly higher than the global average of 38%. In addition, 37% said they have introduced anti-fraud training for employees, compared with 27% worldwide. In total, 68% believe their organisation is in a better place when it comes to fraud prevention than before the incident, compared with 45% in the global survey.

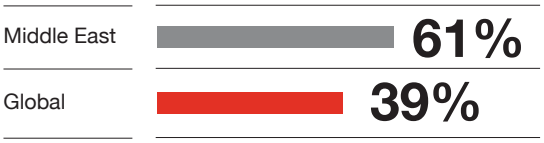
Yet the reality of the rising numbers of organisations experiencing fraud and economic crime is that Middle East, like their global peers, are failing to keep pace with rising and diversifying types of fraud, despite an increasingly strict regulatory environment. Emerging technologies are a key part of redressing this deficit – and here too Middle East and worldwide survey results indicate that organisations still have some work to do.

Middle East organisations financial losses to fraud in the past two years

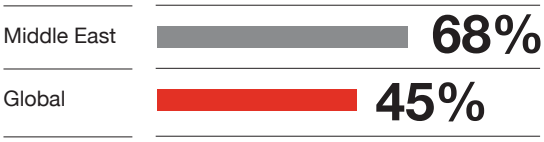


Respondents who said they have implemented or enhanced internal controls following an incident

Respondents who said they have implemented or enhanced anti-fraud policies and procedures following an incident



Organisations that believe they are in a better place when it comes to fraud prevention than before an incident took place



Harness emerging technologies

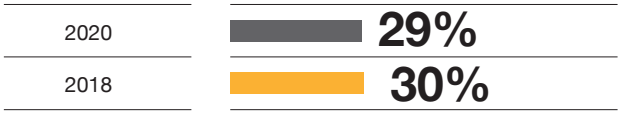
It is notable that only 29% of this year's Middle East respondents have experienced a cyber-crime in the past two years, a slightly lower proportion than in 2018 at 30%. Arguably, this modest decline may indicate improved cyber-security at some organisations. Another interpretation is that a significant and growing number of organisations across the region lack the technological capabilities to detect and combat increasingly sophisticated cyber-crimes, whether committed internally or externally.

In this respect, the answers from our Middle East respondents are in line with their international peers. Some 44% of Middle East respondents said their organisations have a dedicated anti-cyber crime programme, 4% higher than the global average.

The Middle East findings are also broadly similar to the global survey regarding generally weak adoption rates by organisations of alternative or disruptive anti-fraud technologies and techniques. For example, only 31% of Middle East respondents said their organisations are using and finding value in transactions testing and monitoring; 29% report the same for data visualisations and dashboards, and just 11% are finding value in artificial intelligence. This is below the global average of 16%.

However, it is important to note that a single tool or type of technology does not amount to an anti-fraud programme. Organisations must also examine whether they are collecting the right data, analysing it effectively and feeding the findings back into their fraud-prevention programme to make it more robust. Organisations often fail to see the value in technology investments when they fail to provide the right resources and expertise to manage them.

Middle East respondents who said their organisation had experienced cyber-crime in the past two years



Middle East organisations who said they had a dedicated anti-cyber crime programme in place

Middle East organisations who said they are using and finding value in

Act now to be fully prepared

We know that there is a clear link between fraud prevention investments made up front and the reduced cost when a fraud strikes. Our global survey results show that organisations with a dedicated anti-fraud programme in place spent 42% less on response and 17% less on remediation costs than those organisations with no programme in place.

Among our Middle East respondents, 60% have a dedicated programme to fight accounting and financial statement fraud (compared to 44% globally) and 49% have an anti-bribery and corruption programme (39% globally).

Middle East organisations who said they had dedicated programmes in place to fight accounting and financial statement fraud

60% Middle East 2020

44% Global 2020

Middle East organisations who said they had anti-bribery and corruption programmes in place

49% Middle East 2020

39% Global 2020

1. Identify, rank, and address all your risks

Perform robust risk assessments, gathering internal input from stakeholders across the organisation and geographies, to identify risks and assess mitigating factors. These assessments should also incorporate external factors. There is a wealth of information available in the public domain, and ignoring it could potentially result in a big miss. Risks should be assessed at regular intervals (not a 'one and done' approach).

2. Back-up your technology with the right governance, expertise, and monitoring

Recognise that one tool will not address all frauds, and technology alone will not keep you protected. Technology is a vital component of an effective anti-fraud programme, but often is only as good as the expert resources and regular monitoring dedicated to it.

3. Take notice

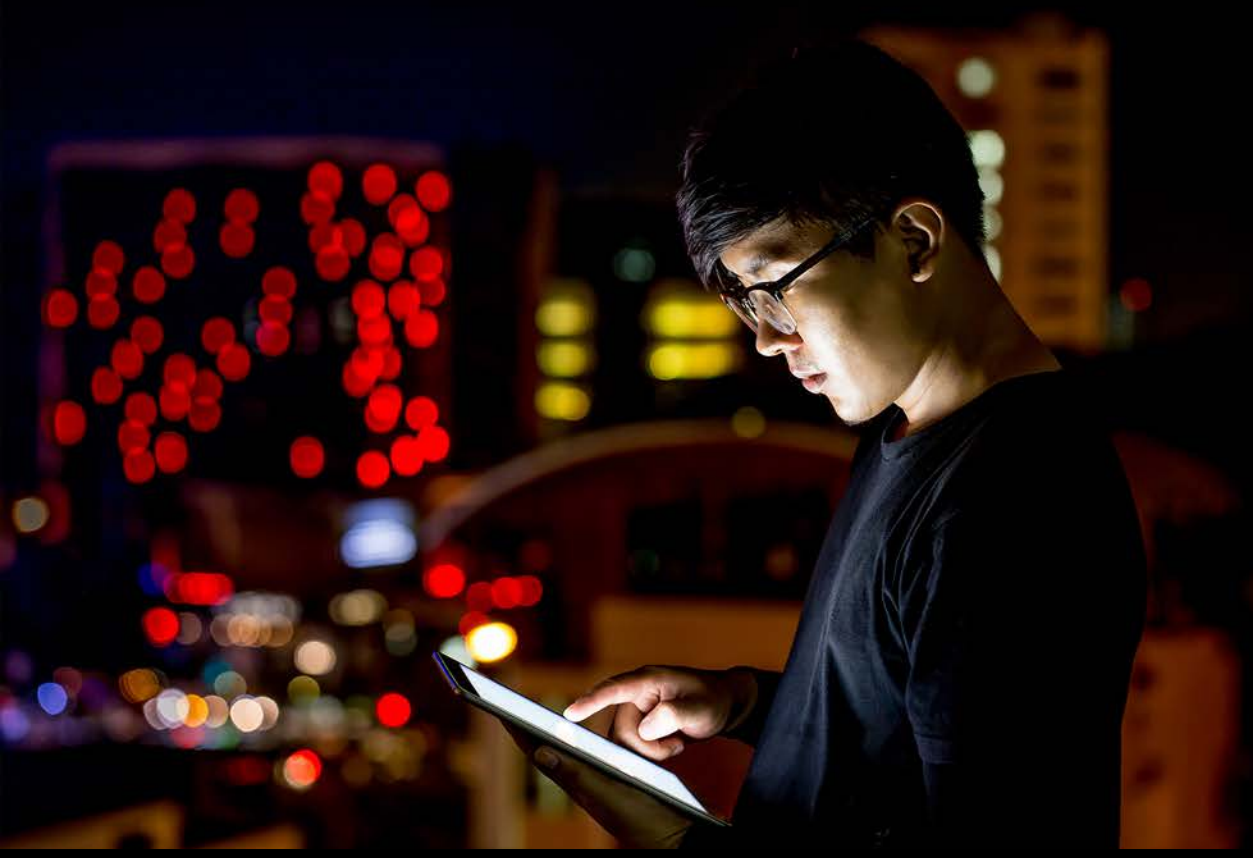
The ability to react to a fraud once identified is an important element of an effective anti-fraud program. Being able to quickly mobilise the right combination of people, processes and technology can limit the potential damage. In some cases, a disruptive fraud may be an opportunity - or a strategic inflection point - to trigger broader organisational transformation for brand protection.

Contact

Achraf ElZaim
Partner, Forensic Services
PwC Middle East
achraf.elzaim@pwc.com

Mahmoud Al Salah
Partner, Forensic Services
PwC Middle East
mahmoud.alsalah@pwc.com

Timur Korshlow
Partner, Forensic Services
PwC Middle East
tkorshlow@pwc.com



About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.
Established in the Middle East for 40 years, PwC has 22 offices across 12 countries in the region with around 5,600 people. (www.pwc.com/me).
PwC refers 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 2000 012020