The fight against economic crime and corruption:

Aligning people, processes and technology to emerge stronger

Contents

Foreword

Alex Tan
Partner and Forensic Services & Risk Consulting Leader,
PwC Consulting Associates (M) Sdn Bhd

PwC has been measuring economic crime and fraud across the globe for over a decade, including in Malaysia. In that time, some marked changes have taken place. This includes the widespread uptake of technology. This is, however, a double-edged sword, that can both prevent and perpetrate economic crime and fraud. Our latest survey (conducted in the second half of 2017) shows that Malaysian companies seem to rely more on a compliance culture rather than controls.

I also note that many Malaysian companies are still failing to perform periodic fraud risk assessments. These are a key part of any fraud and corruption control programme.

On a more positive note, Malaysia's recently published Code on Corporate Governance emphasises the importance of internal controls and the role of boards in setting the tone for controls in the organisation.

Following the recent 14th General Election in Malaysia, we can expect to see the focus on addressing bribery and corruption increase under the new government.

Mobilise your people to tackle fraud together

People

Use technology to stand out in the marketplace

Technology

Assess risks, monitor fraud, and use technology for greater transparency throughout the organisation

Processes

There are **three areas** I would like to highlight this year.

The first, **people** – Malaysian survey respondents feel they have a relatively low level of insight into economic crime in their organisations. 19% said they have insight into certain areas of economic crime in their organisation, while 3% said they have no insight at all. Lack of knowledge, ownership and accountability is often a consequence, hampering efforts to prevent fraud.

Second, **technology** – There is an opportunity for Malaysian respondents to step up their investments in technology to help fight fraud. 36% of Malaysian respondents do not use technology to monitor fraud.

However, Malaysian respondents also surprisingly report a slightly lower incidence of cybercrime this year, compared to 2016 (as covered in our previous report). Companies that can catch up and effectively use new technologies as a risk management strategy stand to differentiate themselves in the marketplace.

Third, **processes** – Besides harnessing technology to mitigate fraud, I advocate regular risk assessment and fraud monitoring. Adopting these processes will provide companies with useful insights, helping them to be more transparent, resilient and agile.

I hope this report gives you and your organisation some useful tools and perspectives to emerge stronger when the next crisis strikes.

Alex Tan
Partner and Forensic Services & Risk Consulting Leader,
PwC Consulting Associates (M) Sdn Bhd

Overview

Economic crime remains a fact of life for businesses in all industries. Our survey indicates that in the last two years, organisations in Malaysia experienced a fraud and crime rate of 41%, slightly lower than the rates in South East Asia (46%) or at the global level (49%).

A fact of life for businesses

It is entirely possible that all organisations experience some form of fraud or economic crime. **59%** of Malaysian respondents have not detected fraud or economic crime yet. The reality is more likely that this statistic measures *awareness* of fraud instead of the *actual occurrence* of fraud.

Respondents

Majority of Malaysia's survey respondents are C-suite executives **(69%)**, followed by heads of divisions **(15%)**, and managers and other executives **(15%)**. Our respondents represent companies from various industries including key sectors of the Malaysian economy such as manufacturing, financial services and the public sector.

Financial losses

22% of the respondents who experienced fraud or economic crime in Malaysia in the last two years reported financial losses of USD1 million or more. This is slightly higher than the wider South East Asian region **(15%)** and globally **(18%)**. Locally, this is a significant jump from **13%** in 2016. Clearly, the scale and impact of fraud has grown significantly in line with technological advancements.

Expanding the study

With the introduction of a new category this year – **business conduct/ misconduct** – asset misappropriation is no longer the most widely experienced economic crime in Malaysia. **45%** of Malaysian respondents report experiencing incidents of business conduct/misconduct in the last two years, while the global average is **28%**, and South East Asia, **39%**. Asset misappropriation is experienced by **41%** of Malaysian respondents - the second most common type of fraud reported.

Non-financial impact

This year, **55%** of respondents reported decline in employee morale as the area of greatest non-financial impact following an instance of fraud. Almost **40%** of respondents ranked reputational harm as having 'high' or 'medium' negative impact on their business.

What is business conduct/ misconduct?

Fraud or deception by companies against the market or general public. Deceptive practices associated with the manufacturing, sales, marketing or delivery of a company's products or services to its clients, consumers or the general public.

Key findings

41% of respondents have suffered fraud or economic crime, up from **28% in 2016**

People

69%

of the most impactful frauds suffered by organisations were committed by internal fraudsters (32% of these perpetrators were senior management)

Bribery and corruption

35%

of respondents reported suffering bribery and corruption in the last two years (an increase from 30% in 2016).

29%

of respondents believe that they have limited or no insight into economic crime in their organisations

Technology

48%

of respondents reported being targeted by cyber attacks in the past two years

85%

of respondents have no plans or are not aware of any such plans to implement AI or advanced analytics to counter fraud

Processes

19%

of respondents have not carried out any form of risk assessment in the past two years

42%

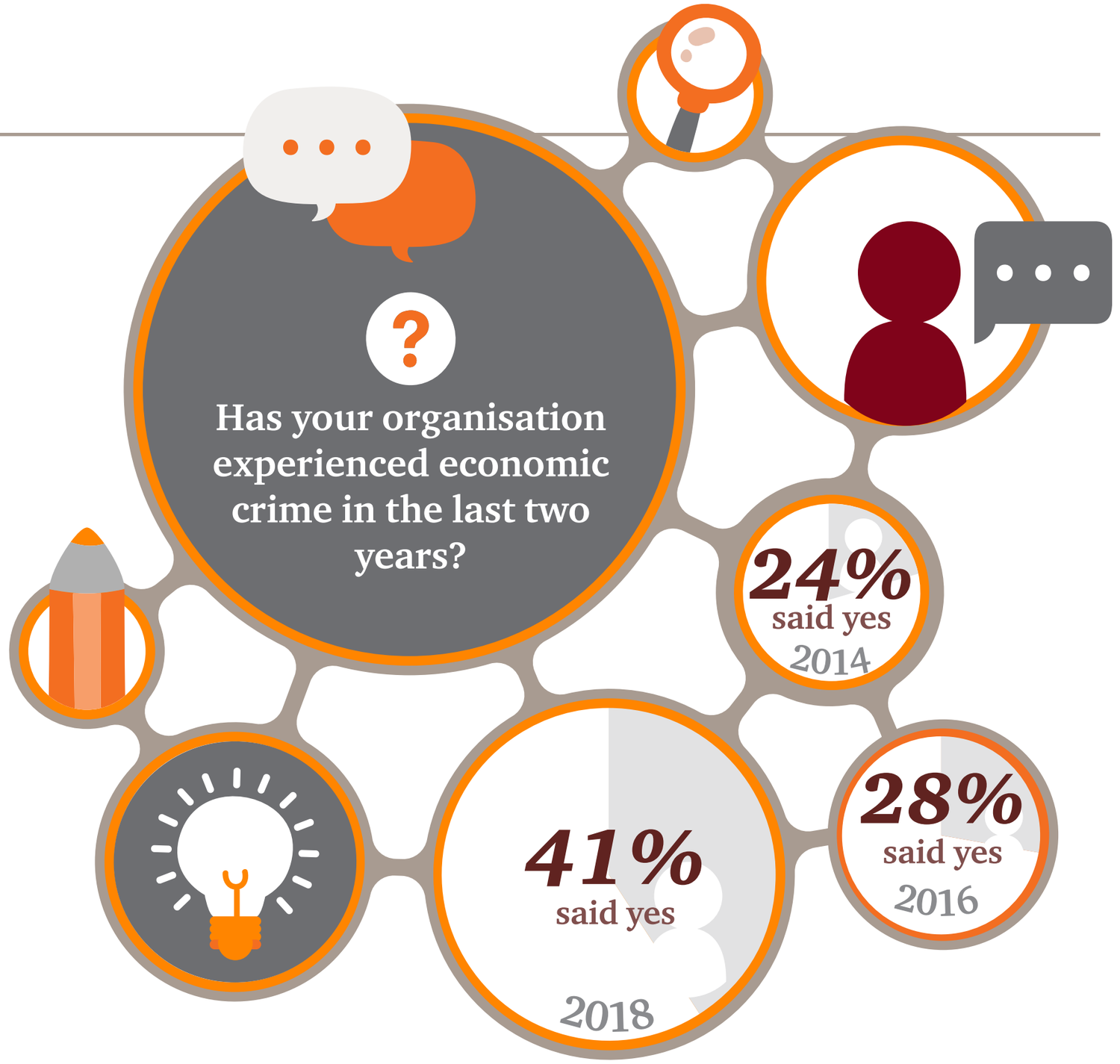
of respondents believe corporate culture to be the most effective strategy in detecting economic crime

What types of crimes are we facing?

Economic crime continues to be a dominant item on the business agenda and no industry, region or size of business is immune. Globally, instances of economic crime continue to increase in frequency and remain a key concern for Malaysian companies.

In Malaysia, 41% of all companies (49% globally) experienced economic crime in the last two years, up from 28% in 2016 (36% globally). However, these numbers are "detected and reported fraud" and not necessarily covering all instances of fraud.

Our survey indicates that Malaysian business leaders appear to be unaware of the potential prevalence of fraud or economic crime in their organisation. Only 23% of respondents say that they have extensive insight into all aspects of economic crime in their organisation.



What types of crimes are we facing?

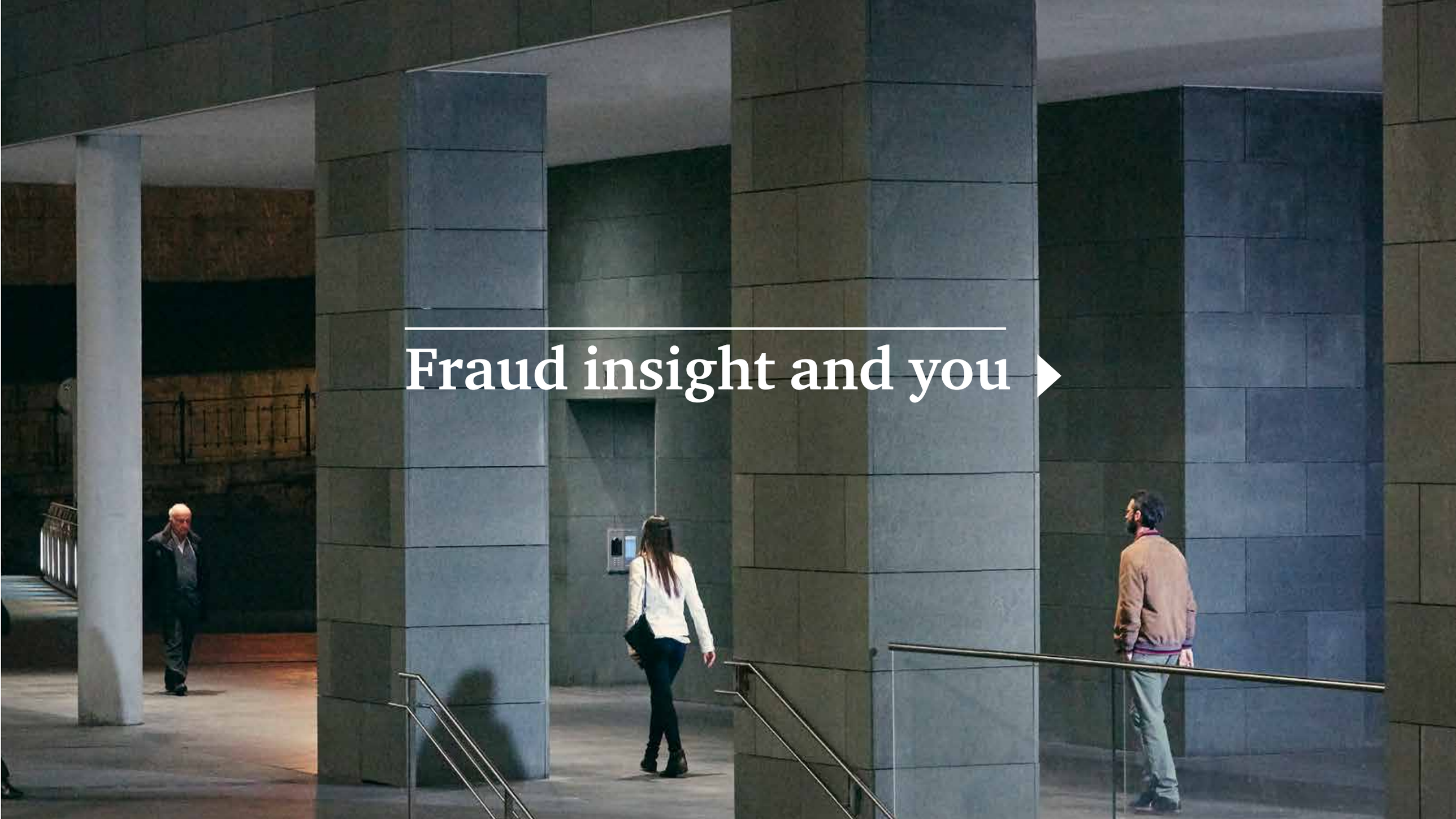
The three most common types of economic crime experienced in the last two years are business conduct/ misconduct (45%), asset misappropriation (41%), and bribery and corruption (35%).

This hierarchy of fraud in Malaysia is consistent with our global survey findings.

Crimes perceived as the highest future concerns:

Asset Misappropriation	18%
Bribery and Corruption, and Business Conduct/ Misconduct (joint position)	15%
Cybercrime	14%

Bribery and corruption ranks as the second highest future concern (i.e. in the next two years) for Malaysian respondents (15%) along with business conduct/ misconduct (15%).



Fraud insight and you

How well do you know your organisation?

The perpetrator – know your adversary

You can't judge a book by its cover when it comes to fraud. A fraudster can sit at the corporate headquarters or work on the shop floor.

The bitter experience of over two-thirds of respondents (69%) surveyed was that the perpetrators of fraud were from among their own staff. While disappointing, this is not surprising, as fraudsters operating within the organisation have a strong understanding of the business. Critically, they know the strengths and weaknesses of the controls in place and if they are in positions of responsibility, they may be able to circumvent these controls.

While fraud can be perpetrated by any level or grade of staff, in South East Asia, 19% of the culprits were senior management. However, in Malaysia, this figure is noticeably higher (32%). This is a cause for concern, as it is often those in senior management that are able to circumvent internal controls. Of the South East Asian culprits, middle management staff accounted for 35% of respondents (vs 26% of Malaysian respondents) while junior management staff accounted for 29% of respondents (vs 13% of Malaysian respondents).

44%

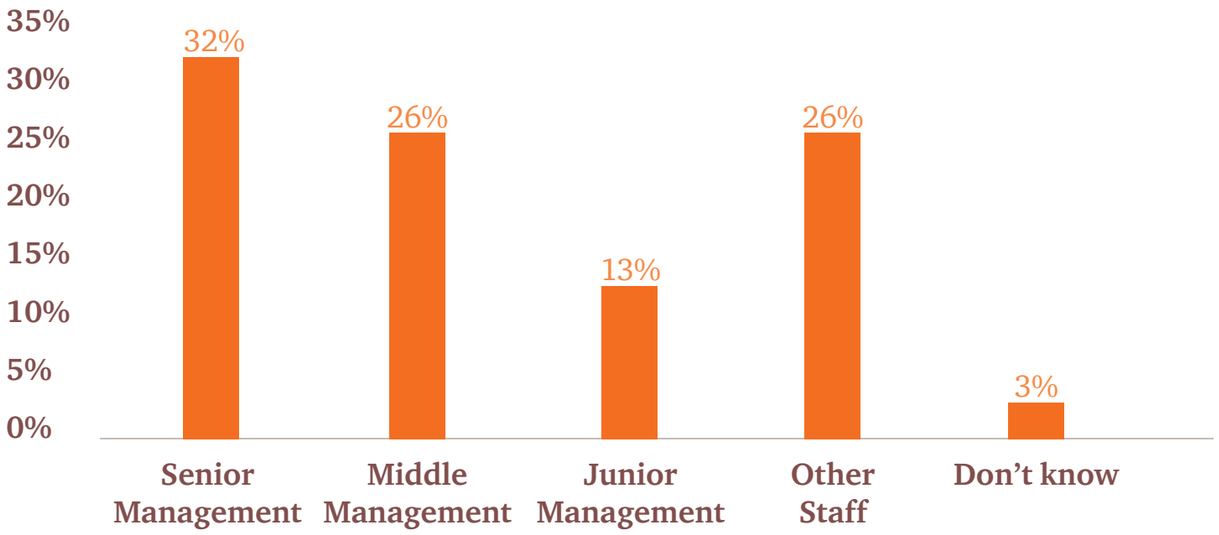
of Malaysian respondents said that internal fraud was most likely committed by personnel from the Operations and Production function.

Globally, internal fraud was also most likely committed by personnel from Operations and Production.

69%

of the most impactful frauds suffered by organisations were committed by internal actors compared with just ***17%*** by external actors.

Who were the main perpetrators of internal fraud in Malaysia?



The drivers of fraud

The fraud triangle

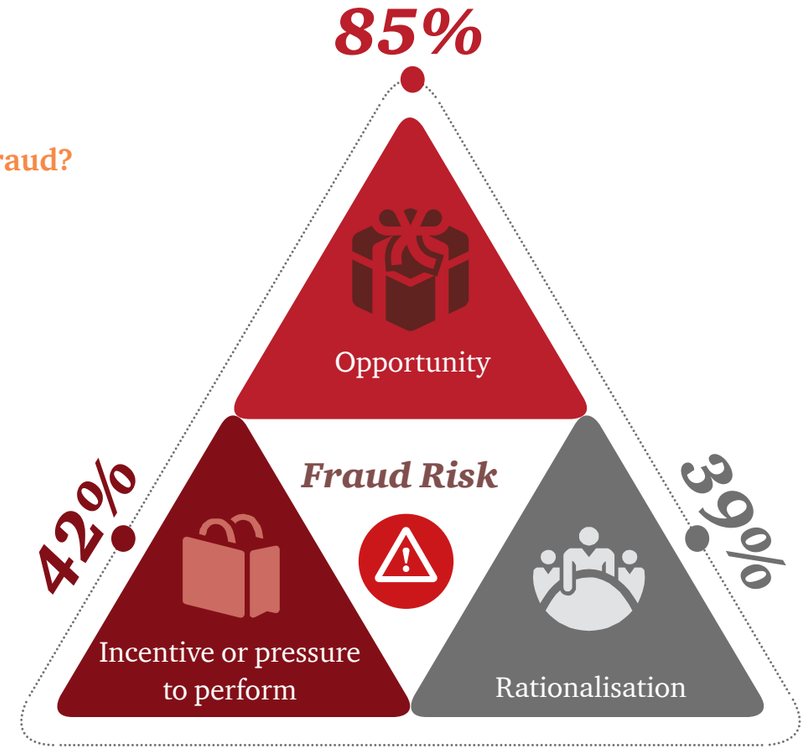
The fraud triangle is a powerful illustration for understanding and preventing the three principal drivers of internal fraud.

It describes the confluence of three conditions when fraud occurs. Perpetrators of fraud feel an **incentive or pressure** (either personal, or professional or both) to engage in misconduct, and identify an **opportunity** to commit fraud.

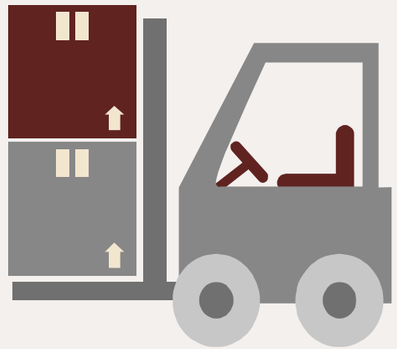
The third corner of the triangle is the perpetrator's **ability to rationalise** or justify their actions.

What makes an employee commit fraud?

To what extent did each of the following factors contribute to the incident of fraud and/or economic crime within your organisation (for those frauds committed by internal actors)?



In Malaysia, **85%** of respondents believe that 'opportunity' is the main driver behind fraud. This is followed by the 'incentive or pressure to perform' (42%) and the ability to 'rationalise' the crime (39%).



Dealing with economic crime: A proactive approach

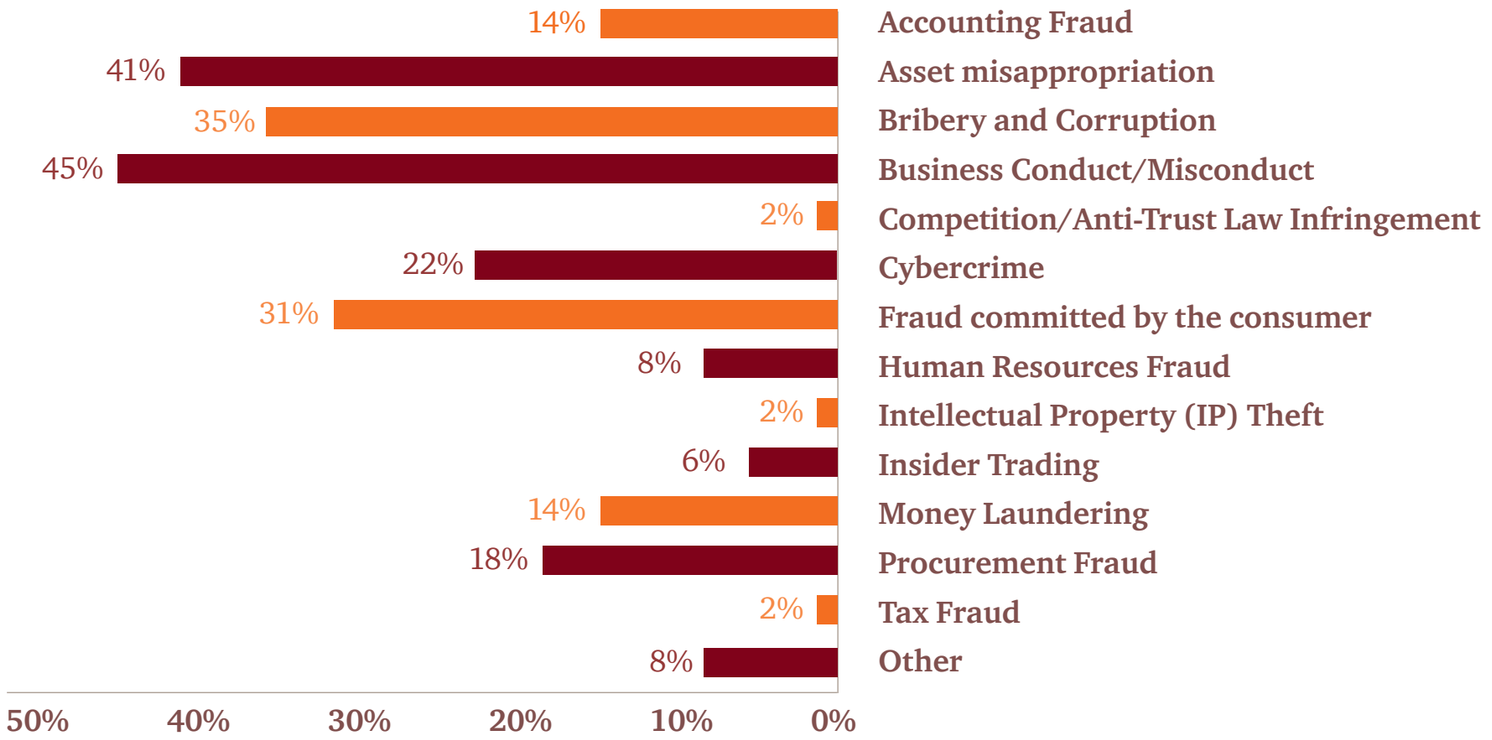
One important measure for identifying fraud vulnerabilities and fighting fraud is to conduct a **fraud and corruption risk assessment**.

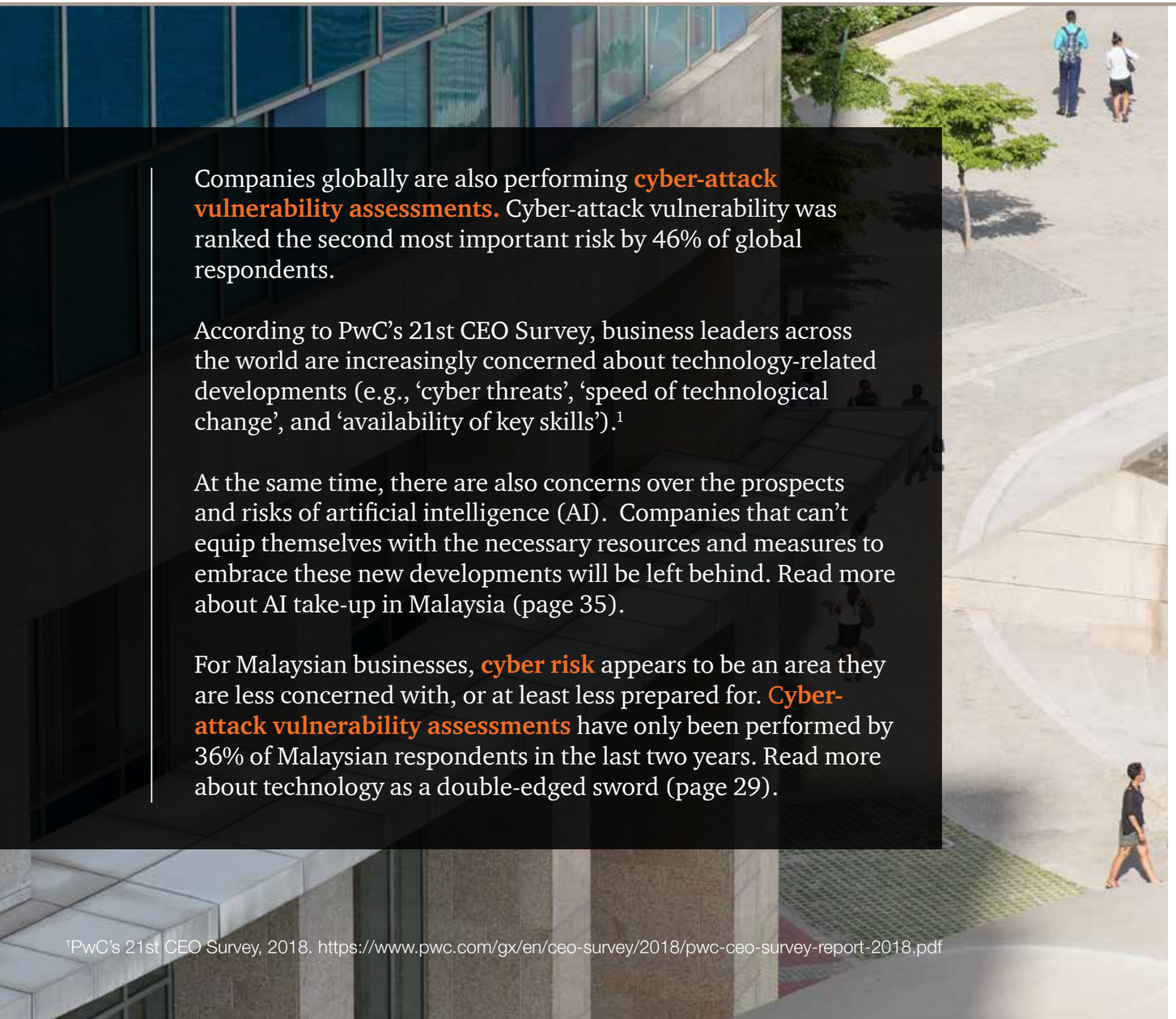
In light of reported weak internal controls among Malaysian companies (which enables more opportunity for fraud), 19% of respondents have not performed any form of risk assessment in the last two years. This is almost double the global average. 5% reported not knowing if a risk assessment had been conducted in their business.

Steps to address risks and vulnerabilities

Those that performed risk assessments, however, make it part of their routine processes, audit plans, or enterprise risk management (ERM) strategy, like their global counterparts.

What types of fraud and/or economic crime has your organisation experienced within the last two years?





Companies globally are also performing **cyber-attack vulnerability assessments.** Cyber-attack vulnerability was ranked the second most important risk by 46% of global respondents.

According to PwC's 21st CEO Survey, business leaders across the world are increasingly concerned about technology-related developments (e.g., 'cyber threats', 'speed of technological change', and 'availability of key skills').[1]

At the same time, there are also concerns over the prospects and risks of artificial intelligence (AI). Companies that can't equip themselves with the necessary resources and measures to embrace these new developments will be left behind. Read more about AI take-up in Malaysia (page 35).

For Malaysian businesses, **cyber risk** appears to be an area they are less concerned with, or at least less prepared for. **Cyber-attack vulnerability assessments** have only been performed by 36% of Malaysian respondents in the last two years. Read more about technology as a double-edged sword (page 29).

[1]PwC's 21st CEO Survey, 2018. https://www.pwc.com/gx/en/ceo-survey/2018/pwc-ceo-survey-report-2018.pdf

However, organisations in Malaysia are investing in improving their business processes to combat fraud, consistent with companies in South East Asia and globally.

50%
of survey respondents rate their level of effort in this area as "high."

Fewer, however, are putting the same level of effort into other anti-fraud efforts such as promoting and verifying ethical decision-making by individual employees. Malaysian companies need to apply a diverse set of measures to succeed in combating fraud.

In the last ***TWO*** years,

19%
of Malaysian respondents have not performed any form of risk assessment

Bribery and corruption keeps rising

It does not come as a surprise that there is a higher occurrence of companies being asked to pay a bribe in **emerging markets** than there is globally.

In South East Asia over the last two years, 23% of companies were asked to pay a bribe (compared to 25% globally). Despite the increase in incidents of bribery and corruption in Malaysia (35%), up from 30% in 2016, in 2018 only 11% of Malaysian organisations reported having been asked to pay a bribe.

While the incidence of bribery and corruption in Malaysia (35%) may be lower than many of our neighbouring countries, it could potentially be due to the fact that many Malaysian organisations were reluctant to report them.

The future of bribery and corruption and how we handle cases of corruption **lie in the hands of every employee.**

Bribery and corruption was the second highest future concern (i.e. in the next two years) for Malaysian business leaders (15%), overshadowed only by asset misappropriation (18%).

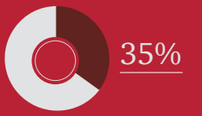
When comparing bribery and corruption to other types of fraud, Malaysian respondents rated it as one of the most disruptive incidents compared to some of our South East Asian neighbours.

Malaysian organisations are not doing enough to protect themselves

Reported incidents of bribery and corruption continue to increase from

2014

2016



2018

It is concerning that some Malaysian organisations appear to be ambivalent about addressing the risks of bribery and corruption.

In the last two years, has your organisation been asked to pay a bribe?

	Malaysia	Indonesia	Philippines	Vietnam	Thailand
2016	6%	27%	25%	Data not available	15%
2018	11% ▲	49% ▲	17% ▼	39%	15% =

% of organisations that reported being asked to pay a bribe

Developments in the regulatory space to address bribery and corruption

On a brighter note, 2018 brings the most significant change to the Malaysian anti-bribery and corruption legislation in years. The imminent implementation of the **Malaysian Anti-Corruption Commission (Amendment) Act 2018** ("the Amendment") will introduce corporate liability in corruption as a legal concept, as well as the concept of the 'Adequate Procedures' defence. This is very similar to the UK's Bribery Act.

The Amendment brings Malaysian anti-corruption legislation to the forefront of the global fight against bribery and corruption. Business leaders must be prepared for this evolving regulatory environment, given the rise of bribery and corruption. Although the Amendment did not apply at the time of the survey, it should help inform Malaysian business leaders' response to bribery and corruption, along with our survey findings.

The recently published global standard **ISO 37001: Anti-Bribery Management Systems,** has also been adopted in Malaysia. ISO 37001 specifies requirements and provides guidance for establishing, implementing, maintaining, reviewing, and improving an anti-bribery management system. A number of government agencies and key companies in Malaysia like Petronas have been certified. The standard is further bolstered by backing from the Malaysian Anti-Corruption Commission. This will show Malaysia's commitment to continuously tackle bribery and corruption as we enter a new era.

Adequate Procedures

The UK Bribery Act 2010 introduced the concept of the 'Adequate Procedures' defence into legislation. If your organisation can prove that it took 'reasonable steps' to prevent bribery and corruption both within the business and in third parties carrying out services on your behalf, then even if corrupt activities occur, you will have a defence in court. These 'reasonable steps' are the Adequate Procedures.

In the context of this report, we define these 'reasonable steps' as:

- Tone from the top
- Risk assessments
- Policies and procedures
- Managing third parties and due diligence
- Communication and training
- Effectiveness testing and continuous improvement
- Monitoring and review

Internal fraud and how it relates to business conduct/ misconduct

This year we have included a new category of fraud: business conduct/misconduct. We define it as economic crime perpetrated by the company, with the fraudulent activity typically affecting customers or suppliers through activities such as deliberate overcharging. This type of crime affected 45% of those respondents in Malaysia who reported experiencing a fraud in the last two years.

Frauds committed by senior management

We have seen a rise in internal fraud perpetrated by senior management across the globe, from 16% of all internal fraud in 2016 to 24% in 2018. With the introduction of business conduct/misconduct as a new category of fraud in this year's survey, we are not able to do a comparison with previous years. However, going forward, the 2018 business conduct/misconduct statistics will serve as a baseline. From our experience, it seems likely that with the increase in fraud committed by senior management, there could be an increase in business conduct/misconduct fraud, given senior management's ability to override internal controls and the pressures faced to produce results.

Based on our observations, business conduct fraud perpetrated by senior management can relate to a range of activities, including the manipulation of accounting records to influence results and deliberate overcharging of customers where contractual arrangements may be vague.

Many businesses are not as alert to the risks of internal fraud, or fraud perpetrated in subsidiaries, compared to the threat of external criminals. However, it is these forms of fraud that are typically the most damaging to brand, reputation and shareholder value. Fraud perpetrated by management particularly presents some unique challenges as they are often harder to spot, especially given management's ability to override certain controls.

Controls and consequences

How to detect fraud? Integrated processes are key

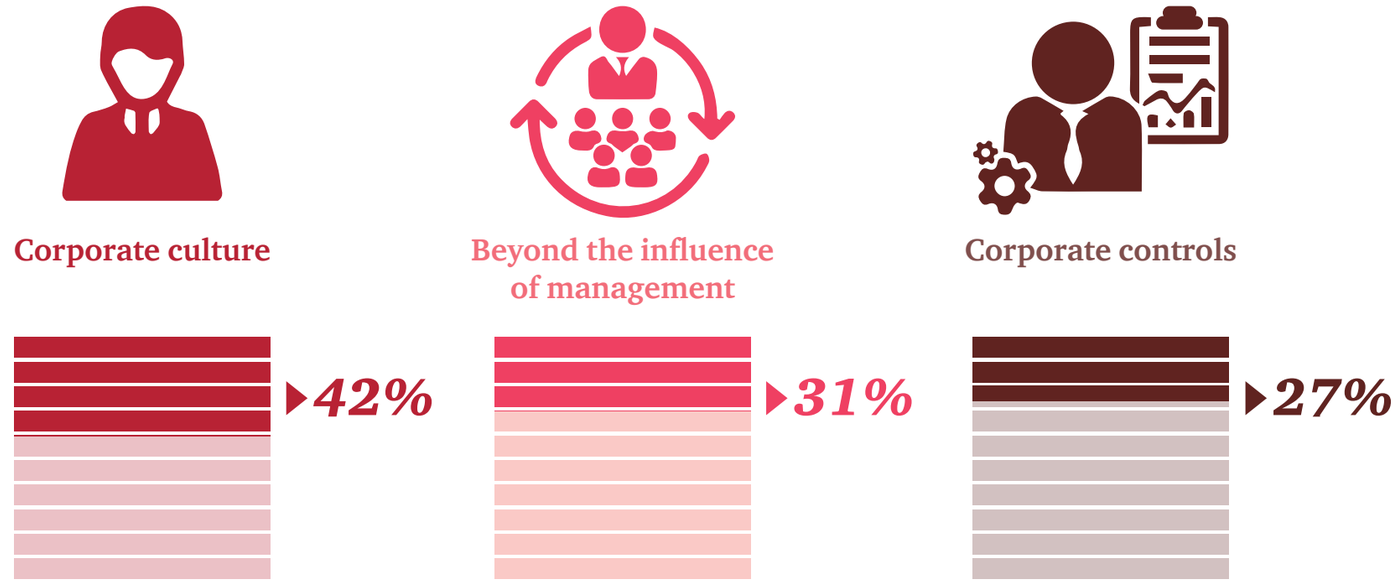
As highlighted earlier, although less than half of Malaysian businesses have reported instances of fraud, the actual number is likely to be much higher – many crimes go undetected. However, for those instances where fraud and economic crime are identified and reported in our survey, some interesting trends emerge.

The current state: A greater focus on culture over controls

In Malaysia, corporate culture plays an important role in detecting economic crime. 42% of respondents view a strong corporate culture which encourages the use of detection methods like tip-offs and whistleblowing hotlines, to be the most effective at rooting out crime.

31% of respondents reported that fraud was detected through methods beyond the influence of management. This includes investigative media, law enforcement and frauds detected by accident. Interestingly, 13% of Malaysian respondents said that fraud was discovered by accident compared to 8% both globally and in South East Asia.

How was the incident of the most disruptive fraud and/or economic crime initially detected?



Just below half of the most disruptive frauds were detected by corporate culture

The findings indicate that the frauds Malaysian organisations are at risk to are consistent with those faced by organisations globally.

As we can see, there appears to be insufficient focus on controls, among Malaysian respondents. Only 27% of local respondents reported that fraud was detected through corporate controls, such as suspicious activity monitoring (15%), internal audit (4%), fraud risk management (4%), corporate security (2%), and data analytics (2%).

The internal control infrastructure available to Malaysian business leaders may be less mature than the infrastructure found in more developed countries. This could explain why only 4% of Malaysian respondents said they detected fraud through internal audit compared to 16% of South East Asian respondents and 14% of global respondents.

The way forward: More emphasis on controls and internal audit

Our experience has shown us that disparate processes (e.g. internal controls) and policies and procedures in companies can often lead to poor internal transparency. This may increase the likelihood of misconduct, as well as the risk that it will go undetected. This builds a strong business case for companies to not only have a strong corporate culture, but to also improve their corporate controls and develop more robust and independent internal audit functions.

How fraud was detected via Corporate Controls

15% Suspicious activity monitoring

4% Fraud risk management (general controls)

4% Internal audit (routine)

2% Corporate security (both IT and physical security)

2% Data analytics

Controls and consequences

The cost of economic crime

Our survey shows us that actual monetary losses can be substantial, but viewing fraud in this manner doesn't give us the full picture of economic crime. Damage from economic crime covers both **financial** and **non-financial losses.**

Financial losses

There are several types of quantifiable financial consequences of fraud including remediation costs, legal fees, actual monetary losses and even criminal penalties. However, despite the fact that non-financial damage may not be quantifiable, for victims of fraud it can be much more significant than just the loss of money, especially in the area of customer trust and reputation.

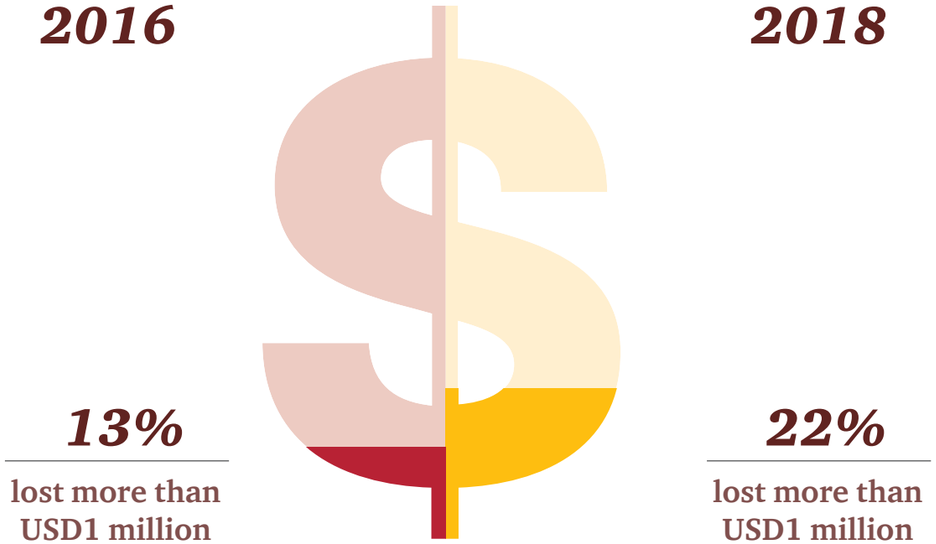
Of the respondents that suffered fraud or economic crime over the last two years:

- more than a third reported losses of over one hundred thousand US dollars (approximately RM400K)
- 48% of Malaysian respondents spent an amount equal to or even more than the cost of the fraud itself to investigate and rectify issues

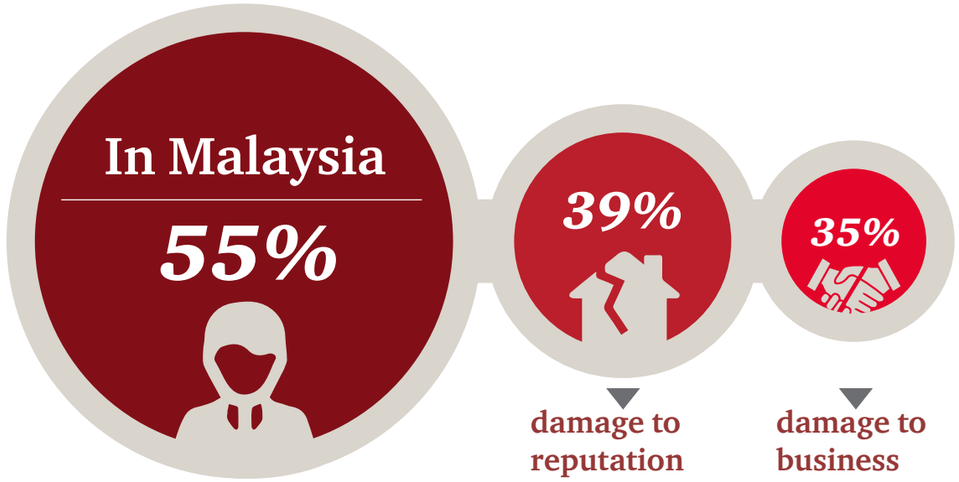
It is worth emphasising that for certain frauds, for example, bribery and corruption, there may not be an immediate financial cost to the organisation.

In the case of bribery, it is merely a channel for attempts (via payment of cash or gifts) to facilitate a process or secure a contract - these may by themselves not be considered "losses" to the organisation. There may be a time lag between the fraud incident and the point at which the financial impact is fully realised.

Financial losses from fraud and economic crime



Non-financial losses



respondents understandably reported **decline in employee morale as the area of greatest non-financial impact***

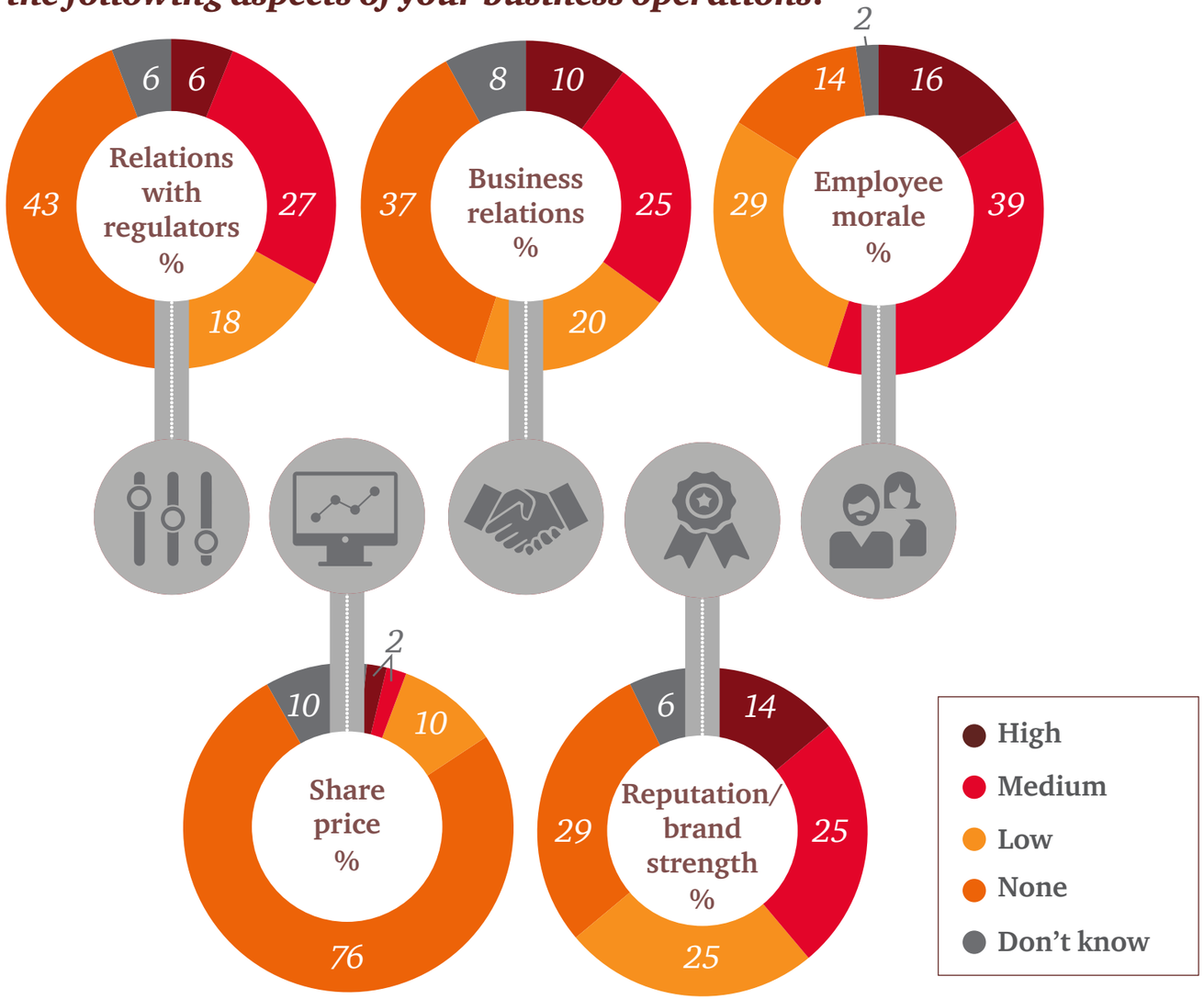
damage to reputation or brand strength in the marketplace*

damage to business relations*

Interestingly, nearly eight out of ten respondents did not think that the economic crimes experienced had any effect on their share price.

* Indicates high or medium level of impact

What was the level of impact of the most disruptive crime experienced on the following aspects of your business operations?



Bad news travels fast: Reputational risk outstrips regulatory risk

Evidently, Malaysian business leaders recognise the reputational risks associated with economic crime, given that, almost

40% *of Malaysian respondents*

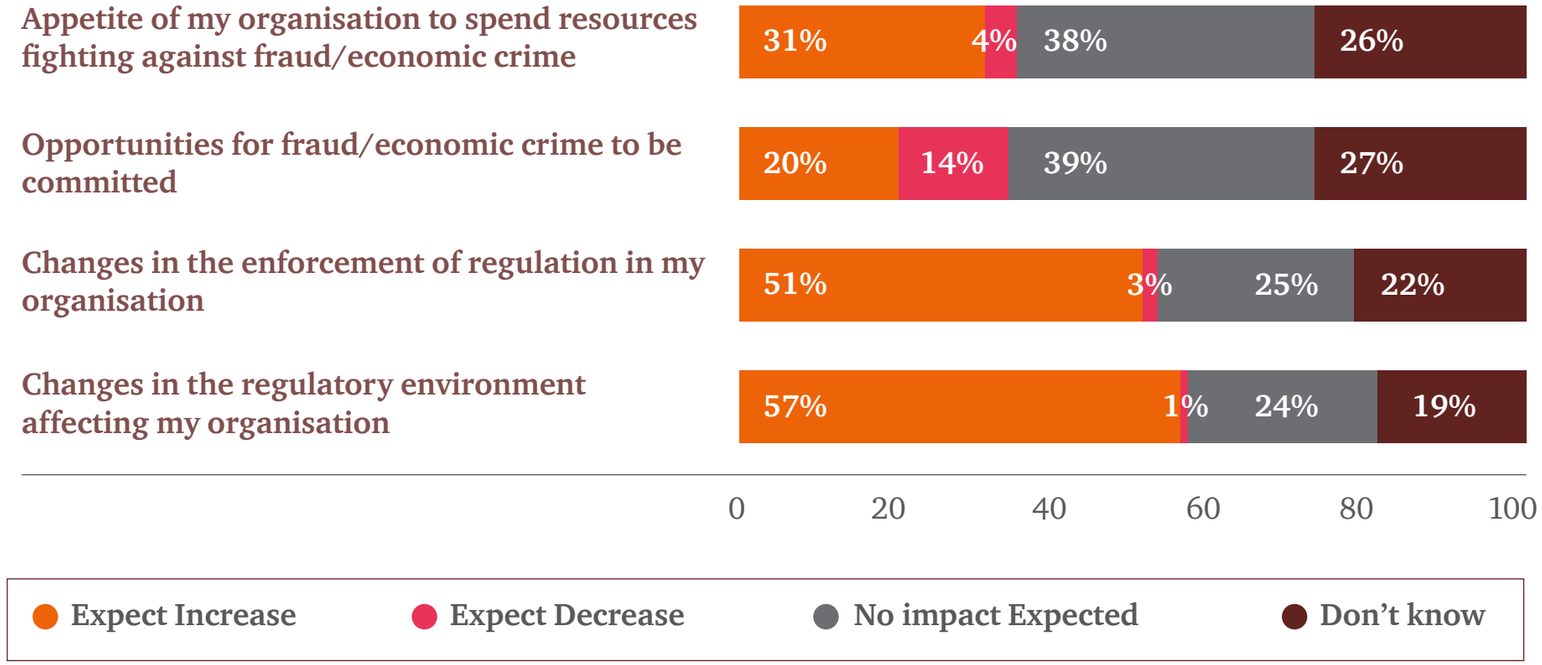
ranked **damage to reputation or brand strength in the marketplace** as having 'high' or 'medium' negative impact on a business. This is reflective of the increasing demand for accountability from both the public and regulators, across the private and public sectors.

Society's rules can change much faster than regulators'. There is little public tolerance for those who break them. Unlike regulators, a company's brand reputation is subject to no fixed jurisdiction, law or due process.

A company that becomes embroiled in cases of fraud or corruption may be punished from all quarters for its perceived inability to respond appropriately – well before the Board or Management has a plan for the next course of action.

On the other hand, regulatory compliance remains as critical as ever. Across the board, regulations and reporting requirements, touching both legal and ethical behaviour, continue to expand. Scrutiny and enforcement are also on the rise. Most Malaysian respondents (57%) expect changes in the regulatory environment to have an increased impact on their organisations over the next two years. A majority of respondents (51%) expect the impact of changes in enforcement to increase in hand with the impact of changes to regulation.

How will recent changes in the geopolitical environment impact your organisation in the following ways over the next two years?



Business ethics and compliance

Compliance is only one part of the solution

If you asked your senior leadership team what their roles are in fighting economic crime, it is likely you would hear a variety of answers. That's a problem. Leaving things to chance because there's no time to address risks, overlaps in responsibility, and grey areas where 'it's not my responsibility'; are gaps that can have a detrimental impact on the overall effectiveness of your fraud prevention efforts, financial performance, and regulatory outcomes.

In Malaysia, 75% of respondents confirmed that they have a formal business ethics and compliance programme in place at their organisations. This is comparable to both the South East Asia region, and globally, where 77% of respondents stated they have such a programme. We believe that the remaining 25% of Malaysian companies would benefit from the adoption of such programmes.

Compliance programmes and processes can only be part of the solution. Investing in the human element of business ethics – building a culture of compliance and encouraging ethical business conduct – is just as important.

As stakeholder expectations for businesses to be ethical and compliant in their operations continue to increase, the companies that do so will get an edge over their competitors, making them more attractive to potential business partners and investors.

Who is responsible?

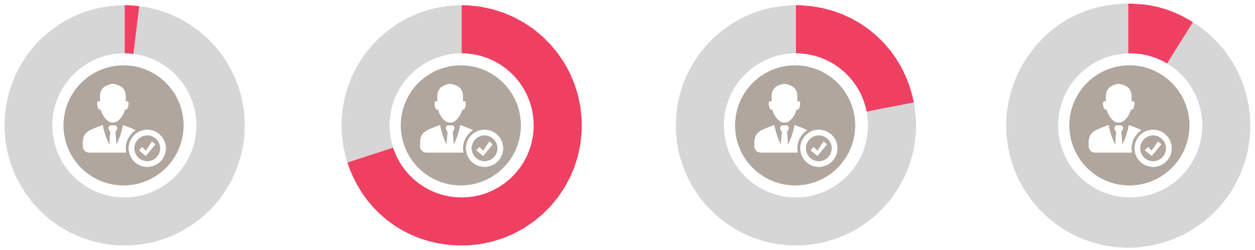
A chief executive is increasingly seen as the personal embodiment of an organisation. So, when ethical or compliance breakdowns happen, these individuals are often held personally responsible – both by the public and, increasingly, by regulators. Whether they're worthy of this or not, one thing is clear: the C-suite can no longer claim ignorance as an excuse.

The majority of our Malaysian respondents reported that C-suite executives are primarily responsible for their organisation's business ethics and compliance programme. This puts a spotlight on how the head office is managing the crisis – and the extent to which they are (or are not) addressing their risks accordingly to emerge stronger.

Just as the reported rate of economic crime has increased since 2016, so too has the amount of funds that companies in Malaysia are spending to fight it:

- 29% of Malaysian respondents said their companies had increased spending on combating fraud and economic crime over the past two years
- 28% of Malaysian respondents said they plan to boost spending over the next two years

How has/is your organisation adjusting the amount of funds used to combat fraud and/or economic crime in the next two years?



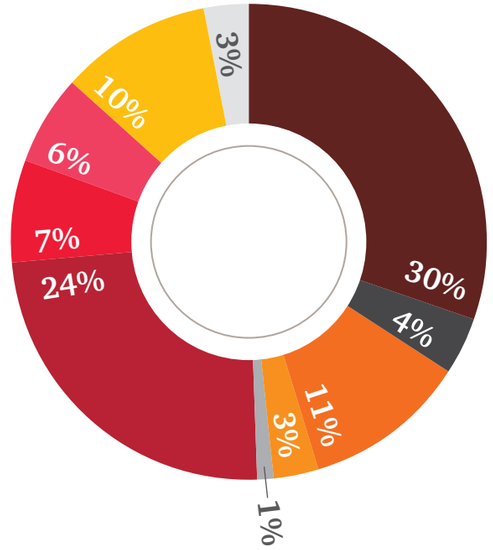
4% Decrease

67% About the same level

21% Some increase

7% Significant increase

Who has primary responsibility for the business ethics and compliance programme in your organisation?



- Chief Compliance Officer
- Chief Executive Officer
- General Counsel
- Chief Risk Officer
- Human Resources Director
- Chief Operating Officer
- Chief Financial Officer
- Other
- Chief Audit Executive
- Don't know

Organisational structure and compliance

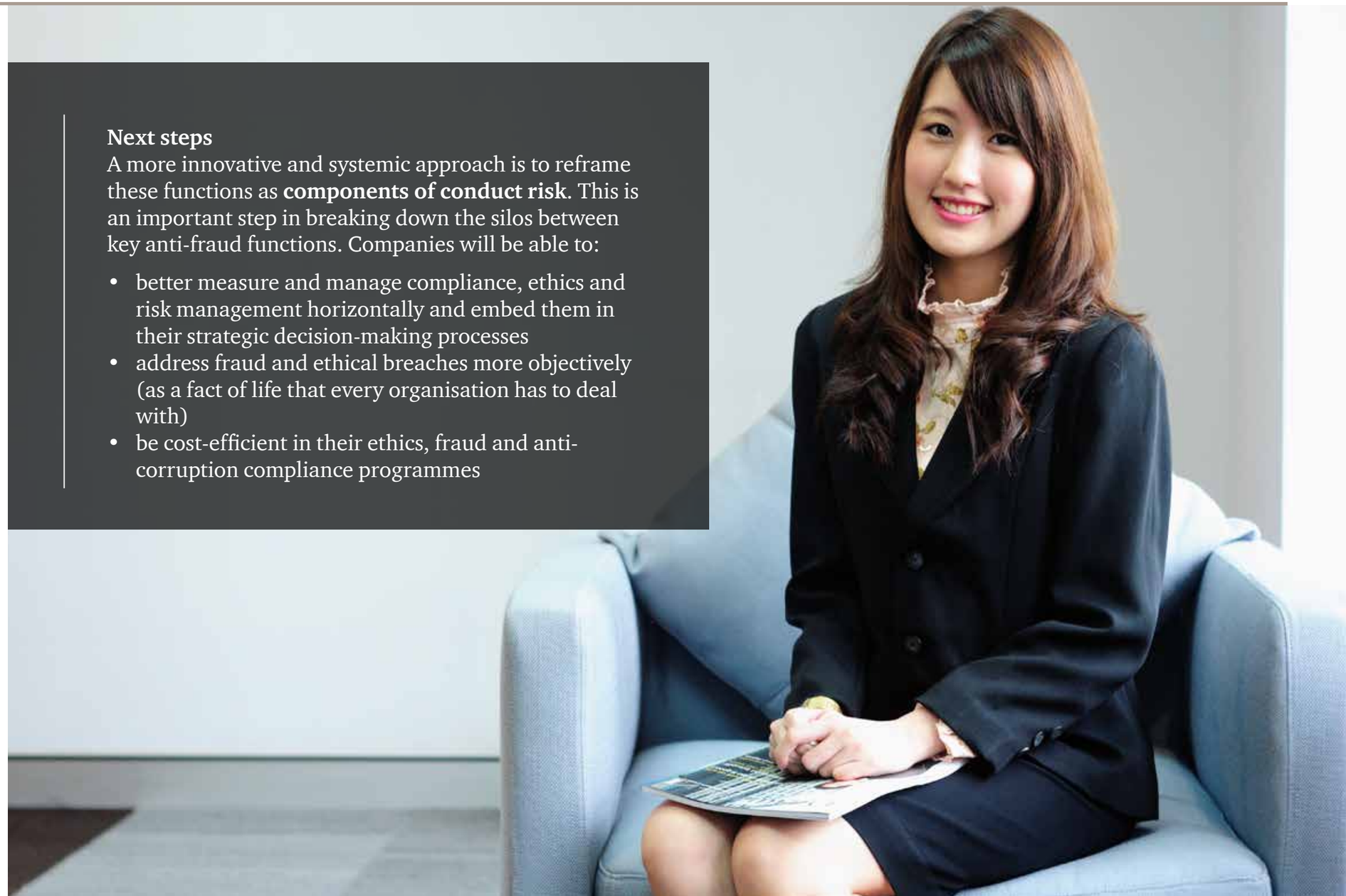
At present, many companies treat compliance, ethics and enterprise risk management as separate functions – sometimes they even exist in separate silos within an organisation. But, like all organisational silos, this means these functions rarely add up to a strategic whole. The parts of an organisation that investigate fraud, manage the risk of fraud, and report fraud to the Board or regulators can become disjointed.

When that happens, operational gaps can emerge and fraud can too easily be brushed under the carpet or seen as someone else's problem. This impacts the overall effectiveness of fraud prevention, financial performance and regulatory outcomes.

Next steps

A more innovative and systemic approach is to reframe these functions as **components of conduct risk**. This is an important step in breaking down the silos between key anti-fraud functions. Companies will be able to:

- better measure and manage compliance, ethics and risk management horizontally and embed them in their strategic decision-making processes
- address fraud and ethical breaches more objectively (as a fact of life that every organisation has to deal with)
- be cost-efficient in their ethics, fraud and anti-corruption compliance programmes



Intelligent use of technology

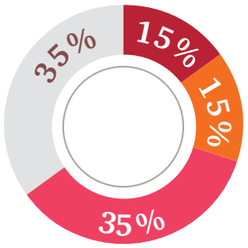
Technology – a double-edged sword

While advancements in technology spell opportunities, they also empower criminals who seek to cause harm. More than ever now, businesses need to minimise risks by investing in their technological infrastructure.

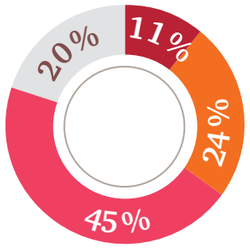
About half of Malaysian respondents reported being targeted by cyber-attacks in the past two years (vs. 64% globally). Incidences of actual cybercrime materialised during this period for 22% of Malaysian respondents. However, only 14% of Malaysian respondents predicted that cybercrime would be the fraud type with the most disruptive impact in the next two years. This is much lower than the expectations of South East Asia (24%) and that of the global average (26%).

Our survey revealed that Malaysian respondents appear to be not taking full advantage of technology in protecting themselves. 26% of respondents don't know if technology is used to monitor fraud and economic crime (and a further 36% confirm they don't use technology at all). This compares unfavourably to the 50% of global companies and 44% of South East Asian companies that do use technology to combat fraud and economic crime.

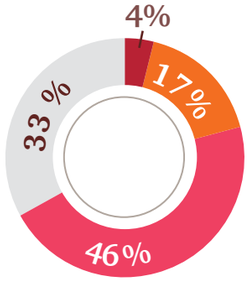
To what extent do you use technology to monitor fraud and/or economic crime in the following areas?



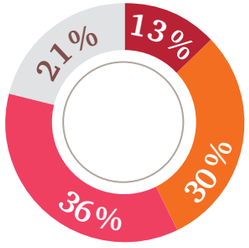
AML Detection



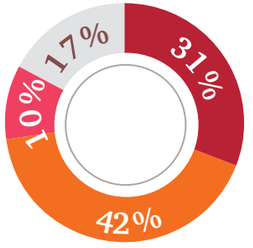
Anti-bribery/ Anti-corruption



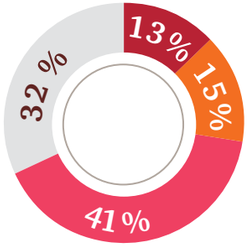
Anti-competitive/ Anti-trust



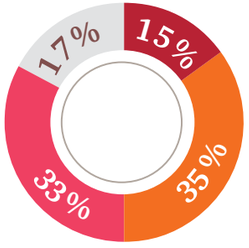
Business Conduct



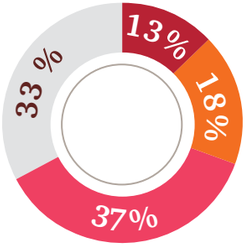
Cyber Attacks/ Vulnerabilities



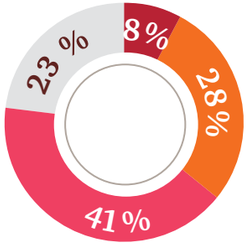
Export Controls



Fraud Detection



Sanction Screening



Third Party Due Diligence

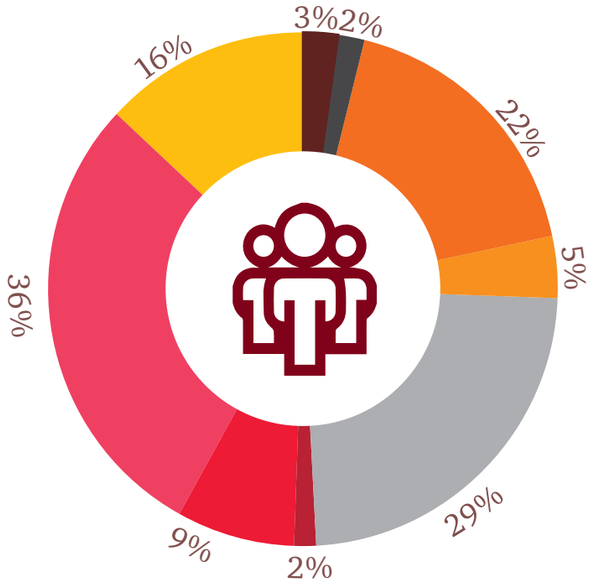
- Primary monitoring technique
- Part of a wider programme of monitoring
- Do not use technology for monitoring
- Don't know

22%

of Malaysian respondents reported experiencing cybercrime in the past two years

Cybercrime: a disconnect between ends and means

In the last two years, has your organisation been targeted by cyber-attacks using any of the following techniques?



- Network scanning
- Brute force attack
- Phishing
- Man in the middle
- Malware
- Other technique
- Yes, but do not know the specific technique
- No
- Don't know

As mentioned, cybercrime continues to rank high on the list of economic crimes reported. It is also important to consider that a significant percentage of those who did not report cybercrime may have unknowingly suffered an event. This underscores the challenge of the threat.

From our experience, many organisations do not have clear insight on whether the data owned or controlled by their organisations have been compromised. In fact, the magnitude of cybercrime may not be felt for years.

Often, the first sign an organisation gets that something systemic is amiss is the detection of a cyber-enabled attack, such as phishing, malware or a traditional brute force attack. The increasing frequency, sophistication and lethality of these attacks are spurring companies to look for ways to pre-empt them. In doing so, this helps them focus more on fraud prevention.

Malware and phishing attacks remain the most common form of cybercrime, in Malaysia, across the ASEAN region, and globally.

Recognising the two forms of cybercrimes

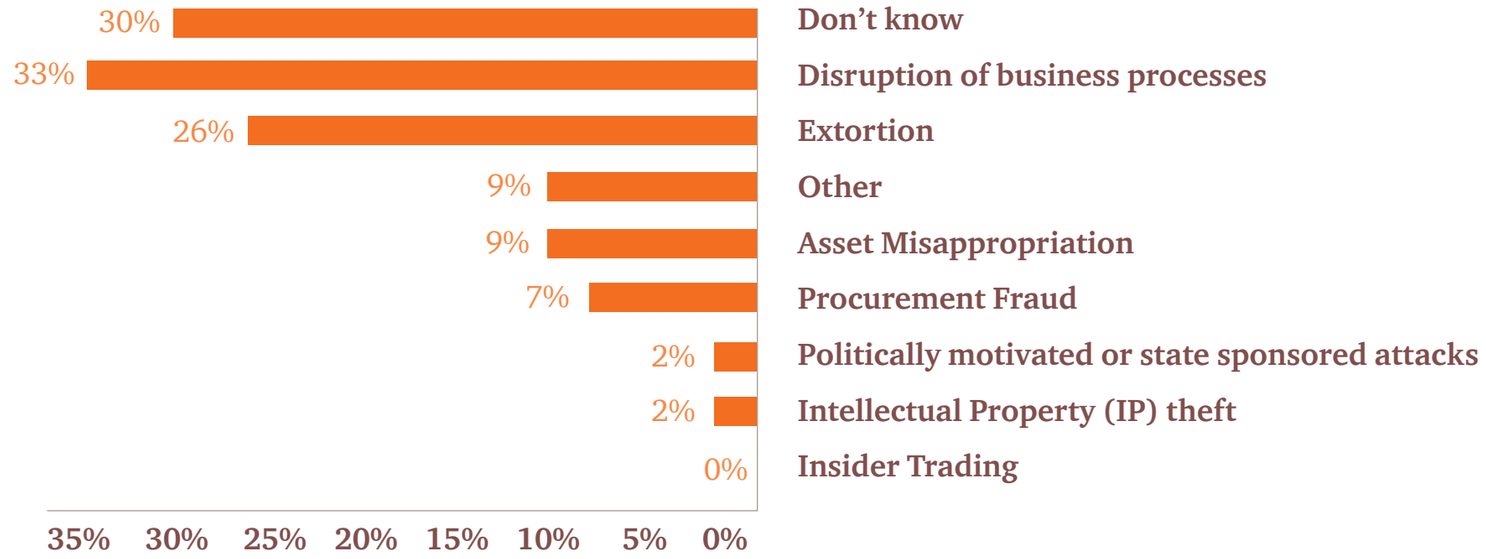
While all digital fraud is fraud, not all fraud is digital. It can therefore be helpful to distinguish two forms of cybercrime:

1. **Digital theft** - The stolen goods, not the smashed door. This type of attack could include stealing cash, personal information, and intellectual property, and could involve extortion, ransomware, or a host of other crimes

2. **Digital fraud** - This type of attack is in many ways more long-lasting and disruptive, because the fraudster penetrates an "open door" (typically, but not always, a customer- or employee-facing access point) and uses the company's own business processes to attack it. To combat this type of fraud, the organisation must use digital methods – both as a vaccine and as a remedy.

8% of survey respondents said that cybercrime was the most disruptive crime, whilst **14%** of respondents said they expected a cyber-attack in the next two years and that it would be the most disruptive

Which of the following types of fraud and/or economic crime was your organisation a victim of through a cyber-attack?



Harnessing technology to address fraud

When Malaysian companies do use technology to counter fraud and economic crime, almost all respondents see the benefits.

75% of respondents agree that technology enables monitoring in real time, and 72% derive actionable insights from their monitoring activities. Most respondents believe that technology provides both strong reporting and robust analytics capabilities.

It's worth noting that the number of Malaysian respondents who confirmed they have a cyber incident response plan in place has also increased, from 35% in 2016 to 57% in 2018. But more needs to be done.

While preventative measures against external economic crimes are critical, it's equally important for businesses to look into how they can protect themselves against fraud committed by internal actors.

An inside job

In our experience, many companies don't actually know where all their own data is. For instance, do you know what company data is held in your employees' smartphones? Do you know where your data is on 'bring your own device' networks?

The threat of intellectual property (IP) leakage is very real. We have worked with organisations that have lost key business information when their senior staff leave with devices holding company IP.

There is an obvious risk of losing your competitive edge when your competitors gain access to your IP. Additionally, your business could suffer reputational damage if word of the leak gets out in your industry, or even the wider public.

Next steps for companies

Evidently, technology exists to curb these risks. The challenge for Malaysian businesses is to identify and adopt the right preventative and detective tools in order to protect themselves, and get ahead of their competition.

25% of respondents do not have a cyber incident response plan

Increasingly we see Malaysian courts willing to grant Anton Piller Orders (APO) – a form of civil warrant to access a defendant's personal records in order to obtain evidence. APOs offer companies a useful tool to recover potential evidence for an investigation, but can require strong legal and technical expertise to get it right. Although the use of APOs may be on the rise, it is only one tool to combat the risks of lost IP.

Incentivising the uptake of technology

36% of respondents said they thought their organisation's use of technology to combat fraud and/or economic crime was producing too many false positives – creating friction

75% of respondents agreed that technology enables continuous real-time monitoring to combat fraud

What is customer friction?

As a customer, it can be reassuring – at first – to know a company is continuously monitoring fraud in the services it provides. But if that monitoring leads to frequent or repetitive alerts, that reassurance can quickly turn to irritation.

This is known as customer friction. And it is a growing challenge for organisations as they seek to strike the right balance between acting appropriately to fraud red flags and being overzealous in alerting their customers.

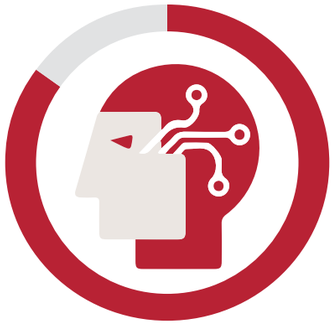
That is not an easy balance to strike – and the margin for error is small. Be too passive and the organisation risks missing a fraudulent transaction, with all the financial and reputational fallout that follows. But be too proactive, and they risk alienating, or even losing, their customers.

Getting this right is important. With the uptake of technology increasing the need for transparency alongside higher customer expectations. Although bad news travels fast, companies that can prove to their customers that they take countering fraud seriously – without causing friction – are more likely to grow and retain their customer base.

Adopting artificial intelligence (AI) to combat and monitor fraud

Machine learning, predictive analytics and other artificial intelligence techniques are some of the technologies available for fraud detection and defence. These tools help companies to monitor, analyse, learn and predict human behaviour.

Such technology can be expensive to buy and to adopt across businesses. Some invest in emerging or disruptive technologies that they don't use optimally. Others adopt technology too late and find themselves behind the curve.



85%

of Malaysian businesses have no plans or are not aware of any such plans to implement AI or advanced analytics to counter fraud

Take-up of AI slow among Malaysian businesses

Few businesses in Malaysia have plans to leverage AI or advanced analytics to combat or monitor fraud and other economic crime. Only 11% of Malaysian businesses are considering implementation, with 3% confirming they already use some form of AI or advanced analytics.

The figures are low, compared to 34% of global respondents and 23% of South East Asian respondents who are at least considering implementing AI or advanced analytics. If businesses are to remain resilient in the face of today's threats, advanced and disruptive technologies must become a core component of any control environment.

Enterprise fraud management solutions, for instance, have grown beyond rule-based fraud detection. The advancement of machine learning techniques coupled with higher computer processing, and access to structured and unstructured data, are allowing for more effective fraud detection.

A multi-layered, technology-driven fraud detection approach can include incorporating authentication methods, and utilising geolocation data, for example. This approach continues to evolve alongside AI like machine learning, natural language processing and image analytics, to name a few.

Sizing the prize – what's the value of AI for your business and how can you capitalise?

+26%

The greatest gains from AI are likely to be in China (boost of up to 26% GDP in 2030) and North America (potential 14% boost). The biggest sector gains will be in retail, financial services and healthcare as AI increases productivity, product quality and consumption.[2]

+14%

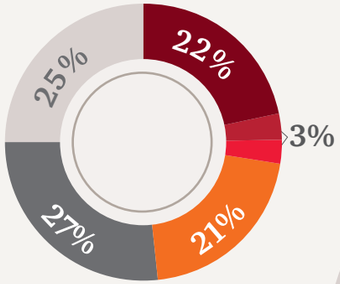
PwC research shows global GDP could be up to 14% higher in 2030 as a result of AI – the equivalent of an additional $15.7 trillion – making it the biggest commercial opportunity in today's fast changing economy.[3]

[2] Source: PwC's 'Sizing the prize' report, 2017, https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf

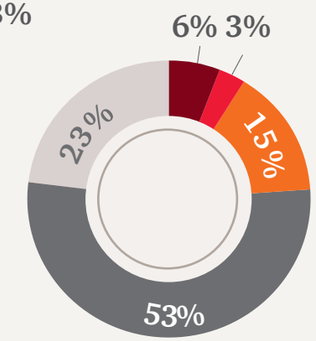
[3] ibid.

Have you considered using disruptive technology to combat fraud and/or economic crime?

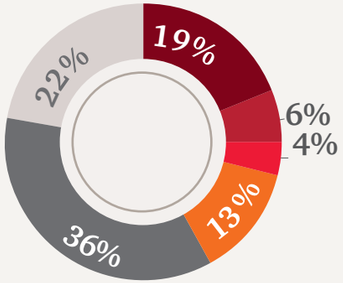
To what degree is your organisation using or considering the following alternative/disruptive technologies and techniques in your control environment to help combat fraud and/ or economic crime?



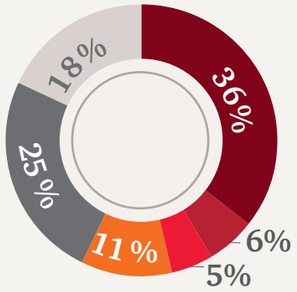
Anomaly Detection



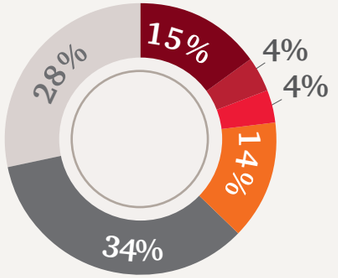
Artificial Intelligence



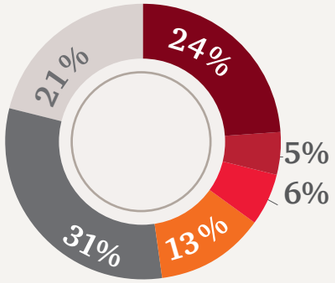
Communications Monitoring



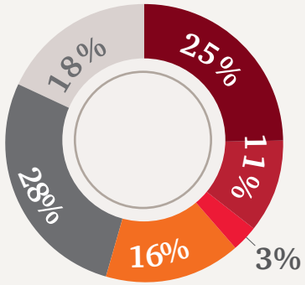
Continuous Monitoring



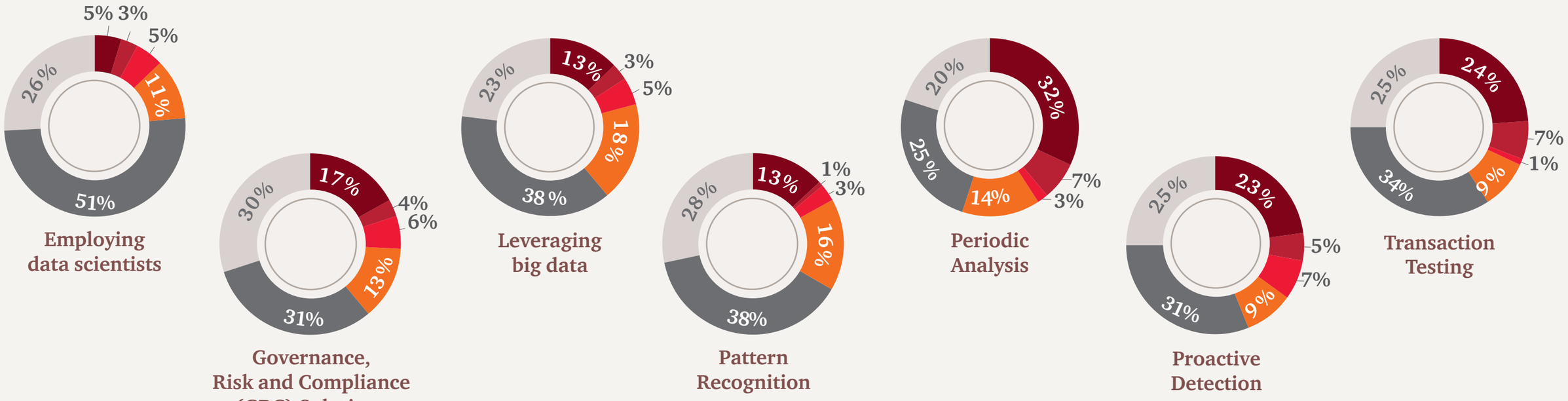
Contract or other unstructured data review



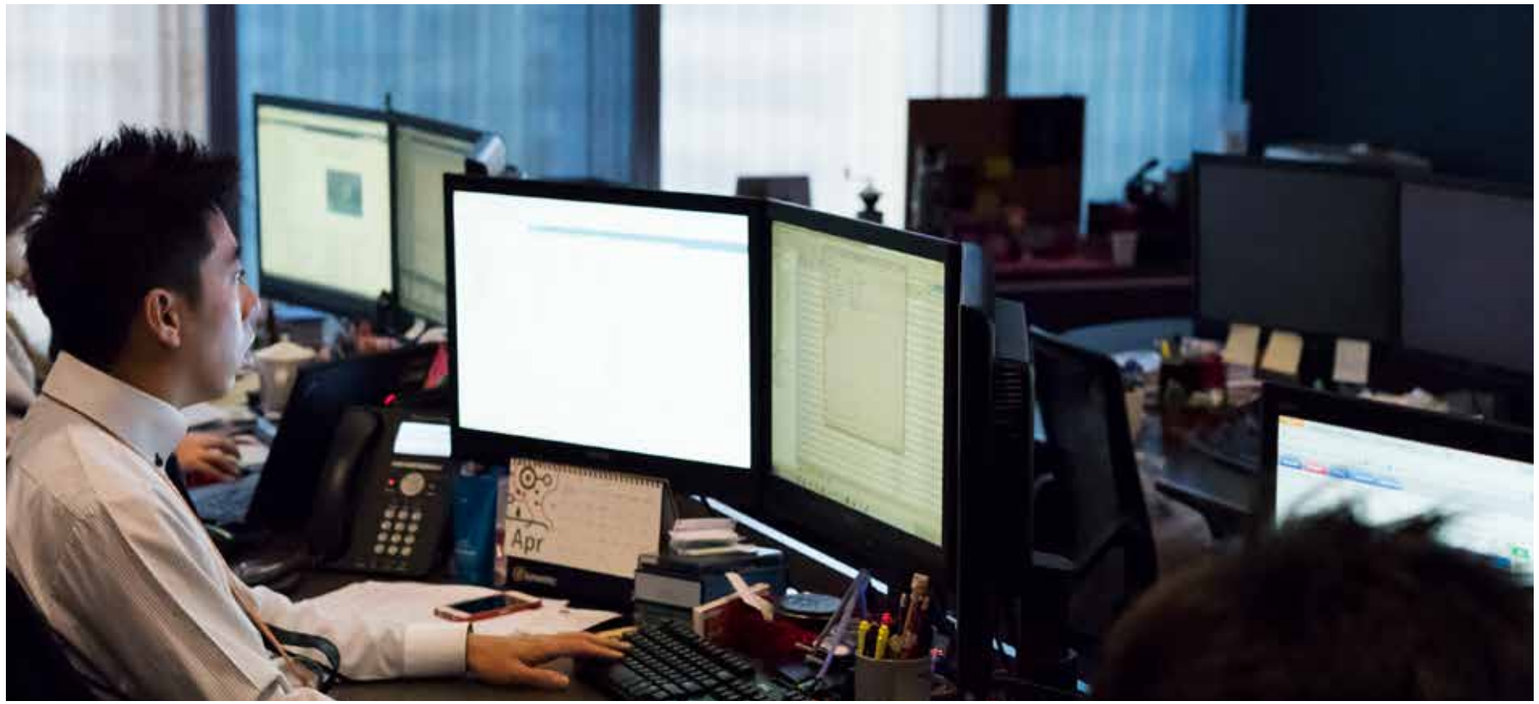
Data Visualisation/ Dashboards



E-mail Monitoring


Using and finding value
Using but not finding value
Plan to implement in the next 12 months
Under consideration
No plans to use
Don't know
5%
3%
5%
11%
26%
51%
Employing data scientists
17%
4%
6%
13%
31%
30%
Governance, Risk and Compliance (GRC) Solutions
13%
3%
5%
18%
38%
23%
Leveraging big data
13%
1%
3%
16%
38%
28%
Pattern Recognition
32%
7%
3%
14%
25%
20%
Periodic Analysis
23%
5%
7%
9%
31%
25%
Proactive Detection
24%
7%
1%
9%
34%
25%
Transaction Testing

Strengthening internal controls with disruptive technology



Interestingly, our survey shows that companies in developing territories are actually investing in advanced technologies at a faster rate than those in developed territories.[4] This is an important step in strengthening internal controls and minimising risk.

The right investment in technology could lead not only to catching up with the rest of the world, but actually 'leapfrogging' other businesses. Taking advantage of the trial and error approaches already taken by many businesses could give Malaysian organisations the opportunity to come out ahead of their global competition.

Just 9% of Malaysian companies said they currently use or are planning to use AI, for example, to combat fraud. This puts us behind both the developed and developing countries' averages (27% and 22% respectively). Investing in disruptive technologies could potentially help us improve our global competitiveness.

The ubiquity of technology creates a double challenge for all organisations: how to find the sweet spot between a technology's effectiveness and its cost, while remaining ahead of the fraudsters.

[4] Our grouping of developed and developing territories was based on the United Nations Conference on Trade and Development classifications. For the purpose of this survey, transitioning territories were treated as developing territories.

What disruptive technologies are Malaysian businesses using?

Proactive detection

Among regional peers, Malaysian respondents were least likely to consider proactive detection, with 31% having no plans to use such tools and a quarter unsure of any plans. 50% of all South East Asian respondents either use or plan to use some form of proactive detection in their anti-fraud toolkit.

Communications monitoring

36% of Malaysian companies have not considered communications monitoring (compared with less than a fifth regionally and globally).

This could be driven by a misinterpretation of local data protection legislation such as the Personal Data Protection Act 2010 (PDPA).

Periodic analysis

32% of respondents find value in periodic analysis, but those who don't use it have yet to consider it. 25% of respondents have no plans to implement any form of periodic analysis, compared with just 11% globally.

Anomaly detection

Malaysian businesses are open to exploring anomaly detection, with 22% of respondents finding value in its use, and a further 24% considering implementation.

Big data

38% of Malaysian businesses have no plans for big data, and 23% are unsure if their business uses it at all.

This contrasts with the 56% of global respondents who are using, or planning on using, big data in their anti-fraud efforts.

Conclusion

What does this mean for you and your organisation?

Whether your organisation belongs to an emerging market, a developed market, or is in the public or private sector, it will always be at risk of fraud. It's not possible to entirely prevent this, but building stronger controls will better arm you in the fight against fraud.

Technology

Investing in and deploying disruptive technologies is vital. Perpetrators of fraud continue to exploit the ever advancing means by which economic crime happens. Any organisation that doesn't keep pace through the uptake of technology, risks being left behind.

Processes

It's true that the tangible value of an up-to-date anti-fraud programme can be hard to quantify, making it sometimes difficult to secure the investments needed. But the opportunity cost – financial, legal, labour relations, regulatory and reputational – of failing to establish a culture of compliance and transparency can be far greater.

People

An effective control environment, while important, is not enough to fight fraud on its own. Malaysian organisations have made good progress in developing corporate cultures that combat fraud, but more needs to be done. Your business needs a culture that rewards the right behaviours, and penalises those that go against accepted practices, or worse – the law. A balance between prevention, detection, investigation and remediation is crucial to any organisation's anti-fraud programme.

You also need to address the increasing expectations of various stakeholders – from regulators and the public to social media and employees. With transparency and the right balance between controls and culture, a company will be well positioned to absorb the shocks of an unexpected event, and ultimately emerge stronger.

3 key takeaways

1

Invest in and deploy the right technologies, empower your people to make the right decisions through your corporate culture, and build robust processes

2

Place transparency at the heart of your corporate purpose; use it to integrate strategy, governance, risk management and compliance.

3

Take a dynamic and proactive approach to economic crime to get ahead of the fraudsters and increase your ability to react in a timely fashion when crisis hits.

Get these right, and you'll be better prepared to respond to fraud, helping you emerge stronger.

Speak to us today

Alex Tan
Partner and Forensic Services & Risk Consulting Leader
PwC Consulting Associates (M) Sdn Bhd
+60 (03) 2173 1338
alex.tan@pwc.com

Peter Viksnins
Director and Core Forensic Services & Anti-Corruption Leader
PwC Consulting Associates (M) Sdn Bhd
+60 (03) 2173 1406
pete.viksnins@pwc.com

Rohit Kumar
Director and Forensic Technology & Data Analytics Leader
PwC Consulting Associates (M) Sdn Bhd
+60 (03) 2173 1786
rohit.z.kumar@pwc.com

	% of respondents	
	2018	2016
Aerospace and Defence	0%	1%
Agriculture	2%	0%
Automotive	5%	1%
Chemicals	2%	0%
Communications	2%	1%
Education	5%	1%
Energy, Utilities and Mining	2%	13%
Engineering and Construction	7%	6%
Entertainment and Media	2%	5%
Financial Services	14%	16%
Government/State Owned Enterprises and Public Services	4%	18%
Healthcare	1%	0%
Hospitality and Leisure	1%	2%
Manufacturing	40%	12%
Insurance	0%	1%
Pharmaceuticals and Life Sciences	0%	0%
Professional Services	2%	8%
Retail and Consumer	3%	2%
Technology	2%	1%
Transportation and Logistics	2%	4%
Real Estate	1%	N/A
Other Industry/Business	2%	6%

Participation statistics

In 2018, we had 124 respondents. Our respondents represented 19 industries. More than 50% of respondents are publicly listed.

Our respondents come from various functions, with a healthy level of executive management, compliance, and human resources staff taking part.

Participation between top and middle management is evenly spread. Companies of different sizes participated, from those with less than 100 employees to those with more than 50,000. The survey was conducted from 21 June to 28 September 2017.

Data resources

Looking for more data?
Visit **www.pwc.com/crimesurvey** - a webpage with many exciting and useful resources for readers wishing to delve deeper into the data, including:

Terminology

Country specific data from around the globe

Additional information and analysis

Links to further relevant materials

Glossary

Terms/terminology	Definition
Anti-competitive/anti-trust	Criminal violations of laws that promote or maintain 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)
Anomaly detection	Identification of outliers, unusual financial activity, spikes in transactions, unexpected fault reports, or surprising results in an organisation
Asset misappropriation	The theft of assets (including monetary assets/cash or supplies and equipment). This includes embezzlement and deception by employees, or theft of company property or assets by outsiders
Communications monitoring	Continuous or occasional monitoring of communication channels – including email, instant messaging, mobile communications and occasionally voice monitoring – for indicators of unusual or fraudulent activity
Cybersecurity programme	The people, processes and technology that assess, build, manage and respond to cybersecurity risk within an organisation
Natural language processing	The use of machine learning to extract computer-readable data from the human voice
Periodic analysis	Data assessment and fraud detection based on analyses of data from set periods (usually of time). Period trends and norms can be identified and used as a baseline in anomaly detection.
Proactive detection	Taking active steps – such as collating and analysing data collected, or performing due diligence on potential business partners – to identify fraud or economic crime, rather than waiting for the repercussions to be felt before the issue is identified
Risk assessment	These are used to ascertain whether an organisation has undertaken an exercise to specifically consider: i. The risks to which operations are exposed; ii. An assessment of the most threatening risks (i.e., Evaluate risks for significance and likelihood of occurrence); iii. Identification and evaluation of the controls (if any) that are in place to mitigate the key risks; iv. Assessment of the general compliance-related programmes and controls in an organisation; and actions to remedy any gaps in the controls. Risk assessments can be broad, running across business assessments, or they may focus specifically on a function, division or process. For example, **fraud risk assessments** and **cyber-attack vulnerability assessments** focus on fraud-specific risks and exposure to cyber-attacks, respectively.

www.pwc.com/my