

Economic crime from the board to the ground:

Why a disconnect is putting Malaysian companies at risk

Global Economic
Crime Survey 2016
(Malaysia report)





When strategy isn't effectively translated into practice, this can be counterproductive in combating economic crime

- Nearly all companies in Malaysia (98%) make it clear to staff that bribery and corruption are unacceptable practices.
- But bribery and corruption in Malaysia still rose sharply, from 19% in 2014 to 30% in 2016.
- Evidently, there is a disconnect between the tone at the top and the reality on the ground.

How is your business strategy aligned with and led by your organisational values?



Economic crime is an obstinate threat

- 1 in 3 Malaysian respondents believe their companies will experience bribery or corruption in the next two years.
- 14% of Malaysian companies were unaware of whether or not they had experienced economic crime.
- 13% of Malaysian fraud victims experienced financial losses in excess of USD1 million.

What are the opportunities to proactively counter economic crime?



Controls must be embedded in organisational culture

- 9 in 10 Malaysian companies believe that opportunity continues to be the driver of economic crime in their organisation.
- 1 in 3 Malaysian companies have not carried out a fraud risk assessment in the past 24 months.

What are the risks your business faces and do you proactively identify and manage vulnerable areas?



Leading Observations

Cyber threats are climbing, but business preparation is not keeping pace

- 61% of CEOs globally are worried about the threat of cybercrime [PwC's 19th Annual Global CEO Survey].
- Less than half of board members globally request information about their organisation's state of cyber-readiness.



Is your cyber-response plan adapting fast enough to the rapidly evolving risk landscape?

Anti-money laundering continues to confound

- Spending on anti-money laundering/countering the financing of terrorism (AML/CFT) controls are expected to drop by as much as 20% in Malaysia, despite ever-increasing risks.
- Less than half of businesses in Malaysia have controls around payments to prevent money laundering.



How will your organisation fare in the face of increasing regulatory scrutiny?



Contents

Foreword	6
.....	
Overview of economic crime	8
.....	
<i>Age-old crimes lead; one pervasive enemy jumps ahead</i>	
<i>Rising financial and collateral damage</i>	
.....	
Profile of a fraudster	12
.....	
Forewarned, forearmed, forward	16
.....	
<i>Bribery and corruption still on the rise</i>	
<i>Procurement fraud – still rampant</i>	
.....	
Cybercrime: A boundless threat	26
.....	
Ethics & compliance: Aligning decision-making with values	30
.....	
Anti-Money Laundering	44
.....	
Appendices	49



Foreword

Over the past decade, we have been studying the economic crime landscape in Malaysia and around the world. The findings have been telling – a significant number of respondents who did not report suffering from corruption, cybercrime and other frauds may have also been victims without knowing it.

Our Global Economic Crime Survey 2016 (Malaysia report) shows that this lack of awareness continues to exist. Malaysian companies are not adapting their risk assessments and control frameworks fast enough to cope with economic crime risks that are evolving in size and complexity.

There is a startling disconnect between the tone at the top and the reality on the ground, particularly for bribery and corruption. 98% of respondents acknowledge that their top level management are sending a clear message that they do not condone bribery and corruption. But the sharp rise in reported bribery and corruption incidents over the past two years suggests that the message may not be getting through.

What is clear is that companies will continue to be tested by the fast-changing regulatory environment, pervasiveness of technology and increasing compliance costs. Consistent engagement with employees as part of a strong zero-tolerance culture towards fraud is key. At the same time, we have to recognise that too much emphasis on enforcement or rules may do more harm than good. Striking an appropriate balance, although harder than it sounds, is critical.

We hope that this report will provide you with some interesting insights into Malaysia's economic crime landscape and prompt some searching questions on how you can protect and defend your business against these threats to stay resilient in such extraordinary times.



Alex Tan

*Senior Executive Director and Forensics Lead,
PwC Consulting Associates (M) Sdn Bhd*



Lim San Peen

*Senior Executive Director and Business Recovery Lead,
PricewaterhouseCoopers Advisory Services Sdn Bhd*

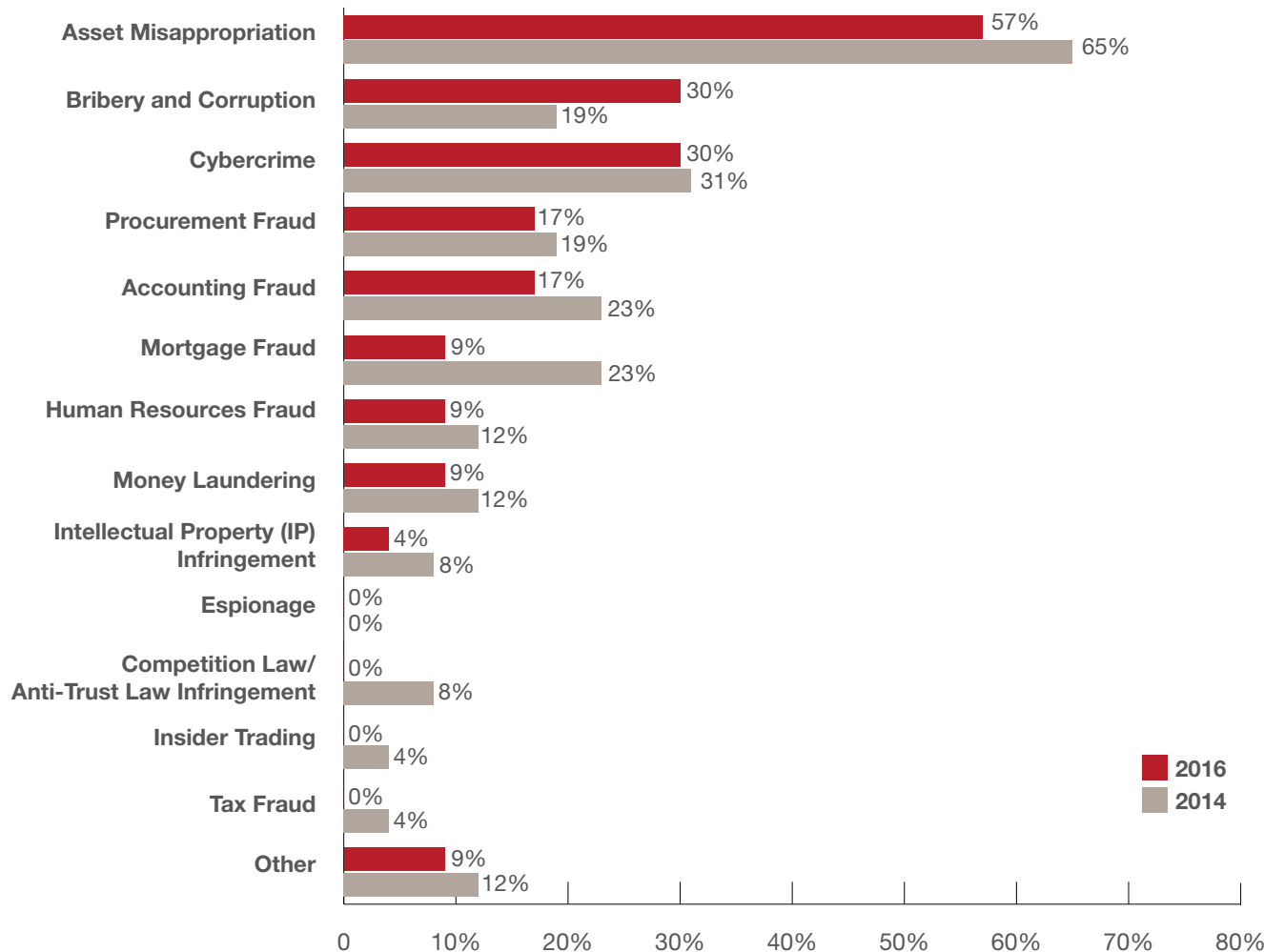


Overview of economic crime

Age-old crimes lead; one pervasive enemy jumps ahead

The most pervasive economic crimes reported by our respondents for 2016:

Fig. 1: *Types of economic crime experienced*



While asset misappropriation, procurement fraud and accounting fraud all showed a slight decrease this year over 2014's statistics, one crime has surprisingly jumped to second place. Bribery and corruption in Malaysia is on the rise, from 19% in 2014 to 30% this year, sharing the second spot with cybercrime.

Asset misappropriation has historically been regarded as the easiest of frauds to detect, thus its prevalence in our survey from year to year is generally predictable. However, we are seeing a decline in reported asset misappropriation incidences both within Malaysia and globally.

We must ask ourselves: are these crimes becoming harder to detect or are we simply becoming less aware of changing threats our businesses face? And the more important question: what should we do about this?



Are some economic crimes becoming harder to detect — or are we simply becoming less aware of the risks our businesses face?

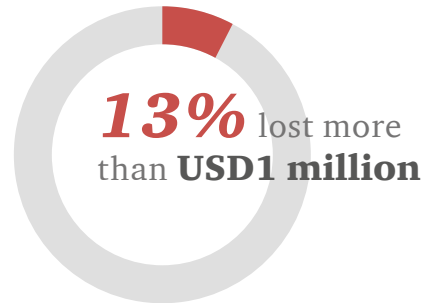
With one in three respondents believing that it is likely that their organisations will experience one of these leading economic crimes in the next 24 months, the time is right for a fresh look.

Rising financial and collateral damage

From a purely financial perspective, 30% of Malaysian organisations who reported being the victims of fraud had losses of more than USD100,000. Those with losses exceeding USD1 million accounted for 13% of our fraud victims. These losses are, however, largely preventable. Appropriate controls and measures to prevent fraud could save your organisation a lot of money. What measures has your organisation taken to mitigate the risk of economic crime? Can you do more?

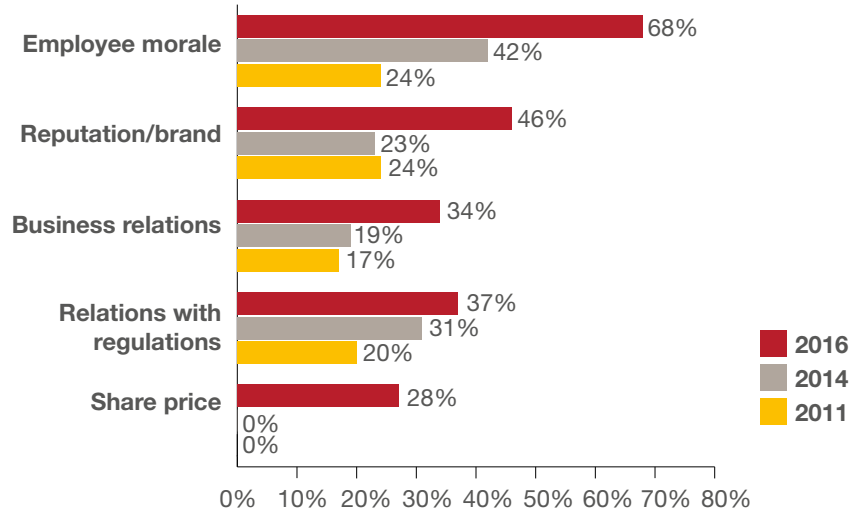
These financial losses do not take into consideration factors that can have a sustained, long-term impact on a business but which are difficult to estimate, such as:

- Reputation damage
- Employee morale
- Status as an employer-of-choice
- Impact on share price
- Relationships with regulators



Most Malaysian companies that have experienced economic crime suffered losses in terms of employee morale, with 68% indicating that the occurrence of economic crime had an impact on employee morale. Nearly half felt negative effects on their brand's reputation, and more than a quarter felt that it had a significant impact on share price. It would appear that companies in Malaysia are aware of the damage that economic crime can inflict.

Fig. 2: *Impact of economic crime*



Non-financial losses appear more strongly felt in Malaysia than other parts of the world. This may in part be cultural sensitivities relating to bribery and corruption, or the types of fraud Malaysian organisations experience. A blind eye toward bribery and corruption among management dampens the spirit in the workplace.

Profile of a fraudster

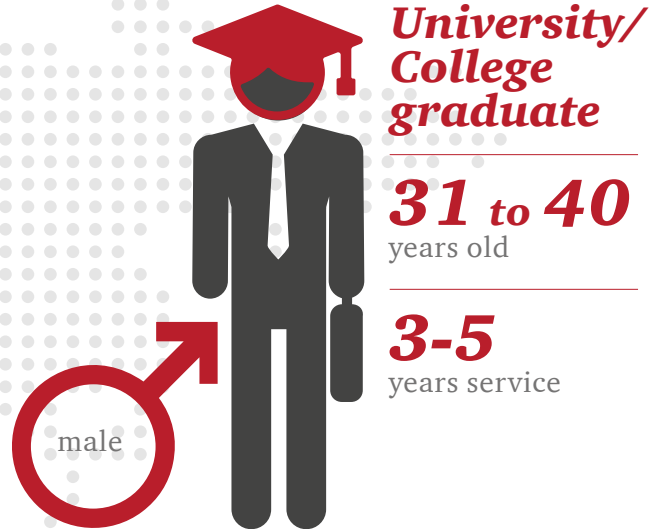
In Malaysia, more than half of fraud perpetrators come from outside the organisation. These external parties include vendors, distributors and customers. Weaknesses in controls and silos within procurement functions result in opportunities for outsiders.

Within an organisation, the typical Malaysian fraudster continues to be male, junior to middle management (66%), aged 31 to 40 years old. They also tend to be well educated, with a university degree or better.

According to these characteristics, an internal fraudster is generally someone with enough experience and autonomy in their position to recognise the controls (or lack thereof) and know where the weaknesses are.



Are these the characteristics of an internal fraudster?



Promoting ethical behaviour: Fear clouds good judgement

Recent research from PwC and the London School of Business on promoting ethical behaviour in the financial services sector shows that a “get-tough” approach to the management of performance has in some cases created a climate of fear which, in turn, leads to unethical behaviours.

The study found that anxiety caused by this blame culture disrupts people’s capacity to make good decisions — and often leads them to behave less well than those who are motivated by the potential positive outcomes of success.

Bribery and corruption

Bribery and
corruption
in Malaysia



from

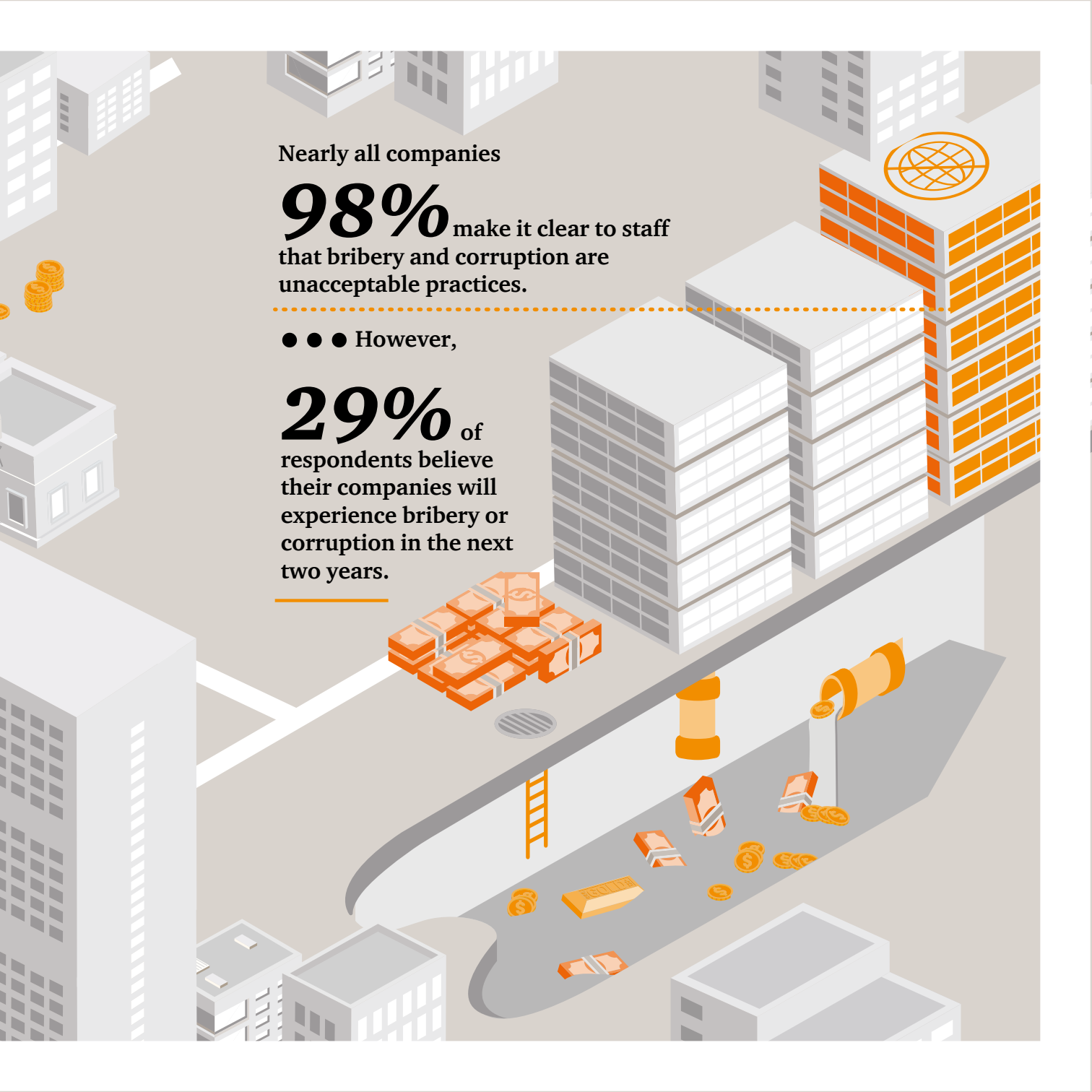
19% in 2014 to
30% this year.



29%

of respondents say they did not
know if their organisation has
been asked to pay a bribe in the
past two years.





Nearly all companies

98% make it clear to staff
that bribery and corruption are
unacceptable practices.

● ● ● However,

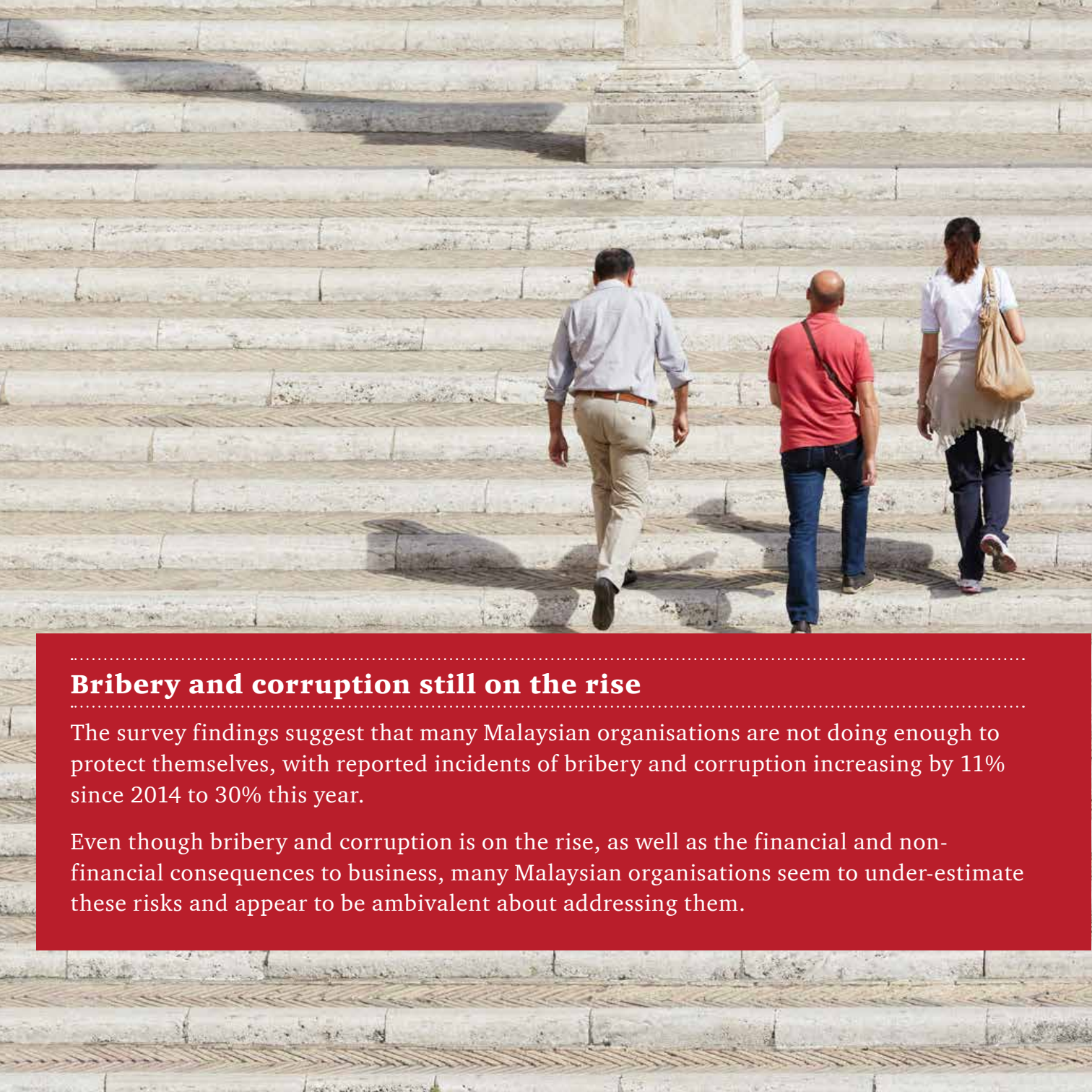
29% of
respondents believe
their companies will
experience bribery or
corruption in the next
two years.

Forewarned, forearmed, forward

Economic crime is ever-evolving, continuously becoming a more complex issue for organisations and economies as a whole. The regulatory landscape, too, is changing, bringing with it numerous challenges to doing business. The business community needs to take the lead in protecting itself, and its stakeholders, from economic crime.

As we discuss in upcoming sections - dedicated to the areas of bribery and corruption, procurement fraud, cybercrime, fraud assessment and anti-money laundering - our survey numbers can help uncover potentially troublesome red flags and trends. They can also serve as vitally important indicators of areas of opportunity for forward-thinking organisations to meet the challenges of a changing world. To be forewarned is to be forearmed for success.





Bribery and corruption still on the rise

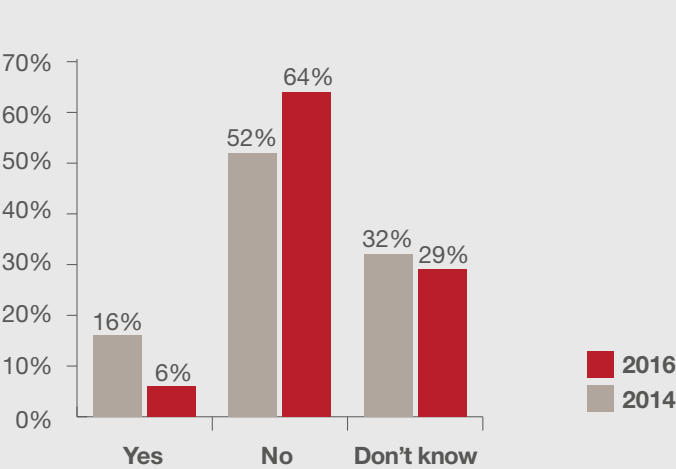
The survey findings suggest that many Malaysian organisations are not doing enough to protect themselves, with reported incidents of bribery and corruption increasing by 11% since 2014 to 30% this year.

Even though bribery and corruption is on the rise, as well as the financial and non-financial consequences to business, many Malaysian organisations seem to under-estimate these risks and appear to be ambivalent about addressing them.



Fig. 3:

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



2. Has your organisation lost an opportunity to a competitor which you believe paid a bribe?

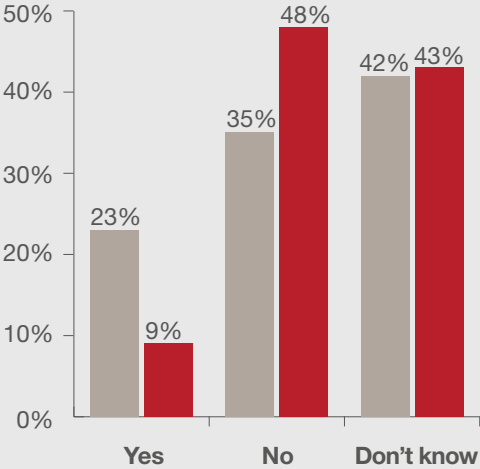
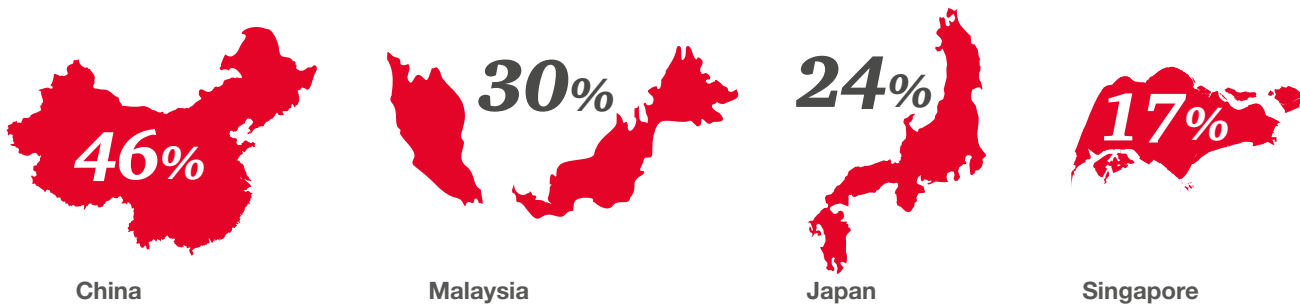


Fig. 4: Bribery reported in Malaysia's top three trading partners



In relation to our top trading partners, Malaysia (30%) occupies the second spot after China (46%), followed by Japan and Singapore in 2016.

In contrast, Malaysia had the lowest reported level of corruption (19%) relative to its three largest trading partners in 2014. With the significant rise this year, our trading partners may see us as a more risky place to do business, and this could have implications to our investment growth. Malaysian companies, in turn, also need to be aware of the corruption risks that exist when doing business with our trading partners.

Though the apparent drop in bribe requests and lost opportunities is heartening, it is concerning that there is a lack of awareness of the bribery and corruption risks that Malaysian companies face. 29% and 43% of the respondents respectively said they did not know if they have been asked to pay a bribe or lost an opportunity to a competitor who paid one.

29% of Malaysian respondents believe their companies will experience bribery or corruption in the next two years. Though this is down from 38% in 2014, organisations in Malaysia should be paying close attention to this risk. Companies should promote a zero-tolerance culture to bribery and corruption through a range of ethics and compliance programmes, as well as undertake regular fraud and corruption risk assessments. Robust and independent reporting methods, such as whistleblower hotlines, are also key. A disconnect between messages from the top and actions on the ground, as we will discuss later, is one of the significant findings of our survey.



As culture and values are the best defence against economic crime, we work with organisations to train their employees and help them develop and communicate a strong message of compliance and speaking up. Too often employees tell us they do not feel supported or empowered to report issues. In order to effectively combat bribery and corruption, your staff are key. If not, your first line of defence becomes the weakest link; an opening easily exploited by would-be criminals.



Procurement fraud – still rampant

More than one in three (37%) of Malaysian companies fear they will experience procurement fraud in the coming two years. By contrast, only 29% of companies globally are similarly worried.

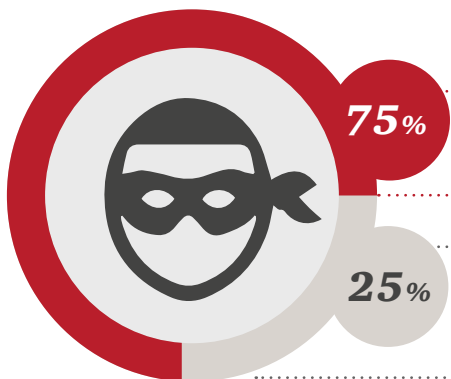
These findings match what we see happening in our clients' organisations. An organisation's procurement function is particularly susceptible to fraud. This in some cases is due to few controls and a lack of understanding of the risks by senior management. These departments tend to have a high level of autonomy and, in some cases, a lack of checks and balances that could prevent would-be criminals from exploiting their employer's weaknesses.

We also find that external actors, i.e. vendors or customers, play a large role in procurement fraud. This is reflected in

our survey, with more than half of local businesses being victims of an external party's criminal activities. However, external actors are nearly always assisted by someone within the organisation. 89% of organisations believe that internal actors within their organisation have the opportunity to commit economic crime. Vendors and customers working closely with your employees will be the first to spot a potential weakness. What has your organisation been doing to limit these opportunities? Are your controls and oversight robust enough to prevent them?



External parties, vendors in particular, are a common source of fraud in our region. 17% of respondents have experienced procurement fraud in the past two years. Of these:



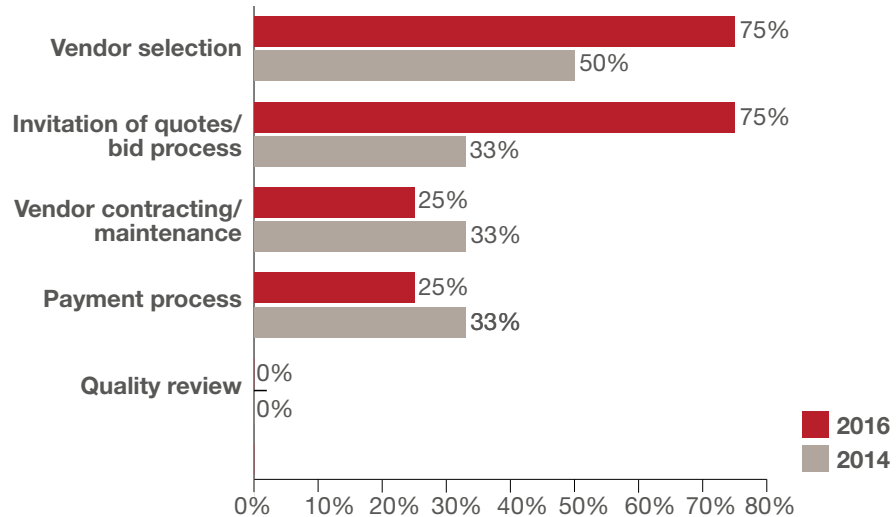
75%

said procurement fraud had occurred during the vendor selection and bid process.

25%

said it had occurred within their vendor maintenance and payment processes.

Fig. 5: Procurement fraud occurrence by stage



Organisations may consider investing appropriate time and due diligence in undertaking a detailed fraud risk assessment across business functions, particularly procurement.



37% Believe that procurement fraud is likely to hit their organisation in the next 2 years.



20% Another 20% weren't sure.

With more than half of Malaysian companies lacking confidence in their procurement fraud prevention measures, prediction could quite easily become reality.

Cybercrime

Almost half of Malaysian organisations

42% see an increased risk of cyber threats.

61%

of CEOs globally are concerned about the threat of cybercrime (PwC's 19th Annual Global CEO Survey).





Only **35%**
of Malaysian respondents have a fully
operational cyber incident response
plan.

More than half
54% of organisations are
unsure of whether or not they are
at risk.





Cybercrime: A boundless threat

Digital technology continues to transform and disrupt the world of business, exposing organisations to both opportunities and threats.

The reality in 2016 is that like every other aspect of commerce, economic crime has, to some extent, gone digital. In a hyper-connected business ecosystem that frequently straddles jurisdictions, a breach in any node of that system - including third parties such as service providers, business partners or government authorities - can compromise the organisation's digital landscape in a variety of ways. What's more, cyber risk now encompasses more than our traditional view of computers: there has been a sharp increase in attack activity involving the so-called 'Internet of Things', including cars and household devices.

Here's the digital paradox: companies today are able to cover more ground, and more quickly, than ever before - thanks to new digital connections, tools and platforms which can connect them in real time with customers, suppliers and partners. Yet at the same time cybercrime has become a powerful countervailing force that is limiting that potential.

And business leaders worry it is holding them back. In PwC's 19th Annual Global CEO Survey, six in ten chief executives ranked cyber threats and the speed of technological change as top threats to growth.

Ready or not

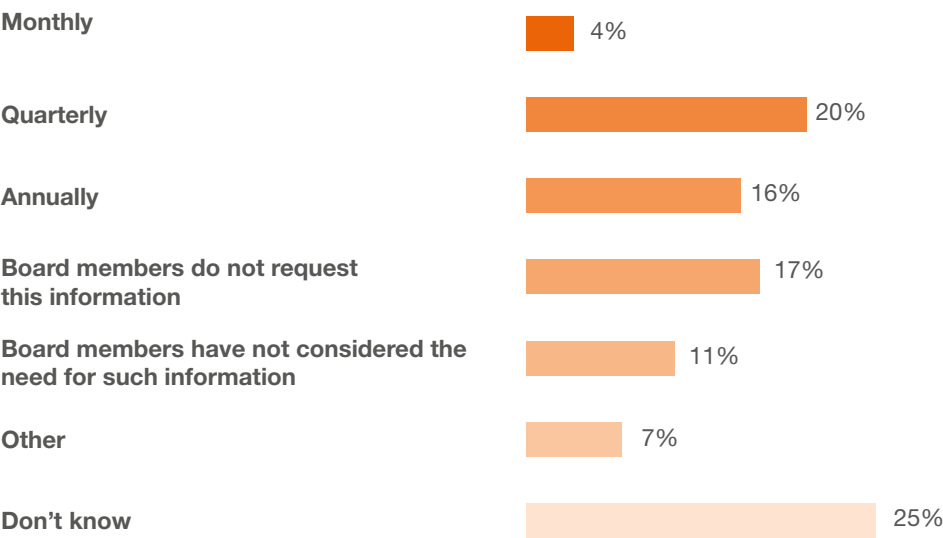
Almost half of Malaysian organisations (42%) see an increased risk of cyber threats. With more than half (54%) being unsure of whether or not they are at risk, there appears to be a lack of understanding of the risks.

Responsibility for redressing cyber vulnerabilities starts at the top. Yet our survey suggests that many boards are not sufficiently proactive regarding cyber threats, and generally do not understand their organisation's digital footprint well enough to properly assess the risks - despite the fact that in several countries, boards have a fiduciary responsibility to shareholders when it comes to cyber risk. Surprisingly, less than half of board members globally actually request information about their organisation's state of cyber-readiness.

What industries are at risk for cybercrime?

Today, all industries are at risk - including some which may have considered themselves unlikely targets in the past. According to PwC's Global State of Information Security Survey 2016, the sector registering the most significant increase in cybercrime activity in 2015 was retail, while financial services - still one of the most attacked sectors - had levelled out, with very little growth in terms of number of attacks over the last 3 years.

Fig. 6: *How often do Board members request information regarding the organisation's state of readiness to deal with cyber incidents?*



Only 35% of Malaysian respondents say that they have a fully operational cyber incident response plan. Three in ten have no plan at all, and of these, nearly half do not think they need one.

With risks on the rise, what is your organisation doing to protect itself from this risk that is not only here to stay, but will get more prevalent and sophisticated?

Ethics & compliance: Aligning decision-making with values

Our survey results show that not only are the number of economic crime risks increasing, so are the complexity of those risks and the role that technology plays in their evolution. This is hardly a surprise in a business environment characterised by growing globalisation, increasingly vigilant enforcement and greater demand for public accountability.

That is why your ability to identify and mitigate compliance risks needs to evolve at a rapid pace. A risk-based approach to ethics and compliance - one that begins with a holistic understanding of your economic crime risks, and an understanding of where your compliance weaknesses are, is a must-have. From that position of clarity, you can create an effective programme that mitigates those risks, and positions you for reaching your business goals. Yet a worrying one in three Malaysian companies have not carried out a fraud risk assessment in the past 24 months, and a further 14% weren't sure if they had or not.





Aside from bribery and corruption, most “traditional” frauds (such as asset misappropriation, accounting fraud, and procurement fraud) have fallen from their 2014 levels. The modest drop in some of these metrics relative to our last survey may be feeding a false sense of security and must be evaluated in relation to the rise in bribery and corruption (which makes the situation more complex). There is a risk that companies may not see the value in investing more resources into ethics and compliance programmes especially if they have not noticed an increase in their experience of economic crime.

Indeed, many organisations have been cutting costs in both headcount and training, or stretching their existing compliance team’s responsibilities to include additional duties. This may be a strategic miscalculation: in many industries and geographies, economic crime risks are not diminishing and a short corporate memory can be dangerous. The deeper point is that while risks and threats are ever-changing, the essence of a successful compliance programme is one that can foresee and address an evolving risk landscape.



Fig. 7: Perceptions of business ethics and compliance

There is a clear Code of Conduct covering organisational values and expected behaviours



Organisational values are clearly stated and well understood



There are confidential channels for raising concerns



Ethical business conduct is a key component of our HR procedures



Senior Leaders and Managers convey the importance of ethical business conduct in all that they do



Concerns can be raised confidentially, without fear of retaliation



Training on the Code of Conduct (and supporting policies) is provided regularly



Irrespective of level, role, department or location, disciplinary procedures and penalties are applied



Irrespective of level, role, department or location, rewards are fair and consistent



Agree strongly
 Agree
 Neither
 Disagree
 Disagree strongly



A disconnect

In Malaysia, respondents felt that their top level management are sending a clear message with an impressive 98% agreeing that bribery and corruption are not legitimate business practices. Yet, in the past two years, incidences of bribery and corruption have risen by 11%.

Do these lapses indicate that such programmes are not keeping up with changing business risks? That they are sending mixed messages? Or is there a deeper reason for this apparent disconnect?

Refer to the case study on the next page to learn how a company reassessed its communications approach on fraud.

The numbers point to a perception gap between what CEOs and boards say and what's actually happening in the business. According to our survey, middle managers remain the most likely to commit fraud and those most likely to feel that values are not being clearly stated, or that incentive programmes are not fair.

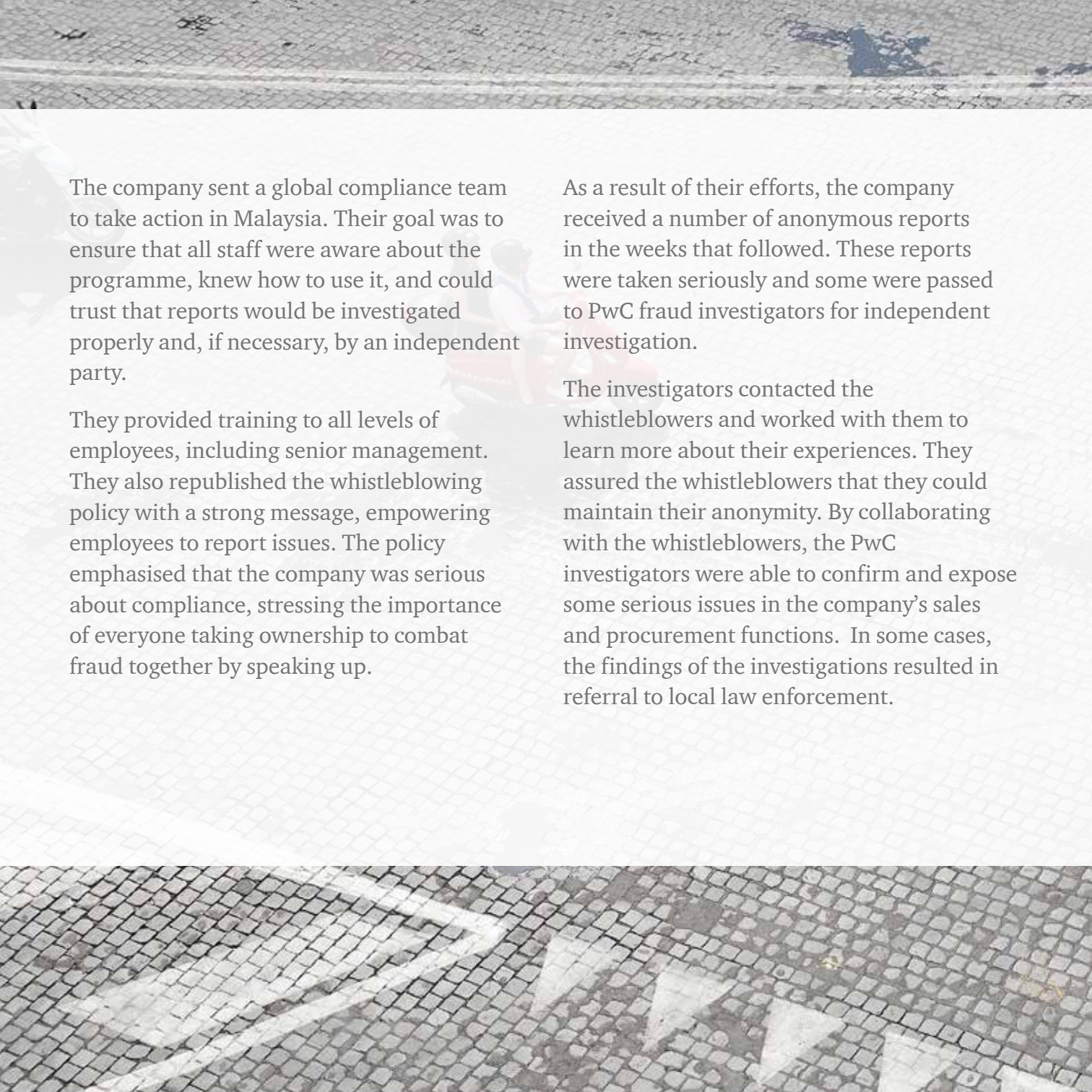
PwC's 19th Annual Global CEO Survey corroborates this theme of a gap between intention and execution. Of the top threats facing organisations, the percentage of chief executives globally naming bribery and corruption saw the greatest increase (from 51% last year to 56%). A lack of trust in business was another reported key threat, underscoring the importance to leadership teams of having a sophisticated, credible corporate ethics programme.

Aligning strategy and action:

A case study

What if you already have a strategy to combat economic crime, but it is not yielding results? The reality is that having a strategy is not enough. Communicating the company's stance on fraud to employees clearly and through the right channels is critical. One company got it right by revamping its whistleblower programme and reframing its communications on fraud.

The company in question, a multinational, found their globally implemented whistleblower programme to be largely effective. Reports of fraud, misconduct, and other inappropriate behaviours were being received by global headquarters on a regular basis from other territories. These reports were being investigated, coupled with remedial action being taken. The whistleblower hotline was used regularly at a global level, but was virtually unused in the Malaysian office. Why was this the case? They found that the system was not trusted by employees in Malaysia.



The company sent a global compliance team to take action in Malaysia. Their goal was to ensure that all staff were aware about the programme, knew how to use it, and could trust that reports would be investigated properly and, if necessary, by an independent party.

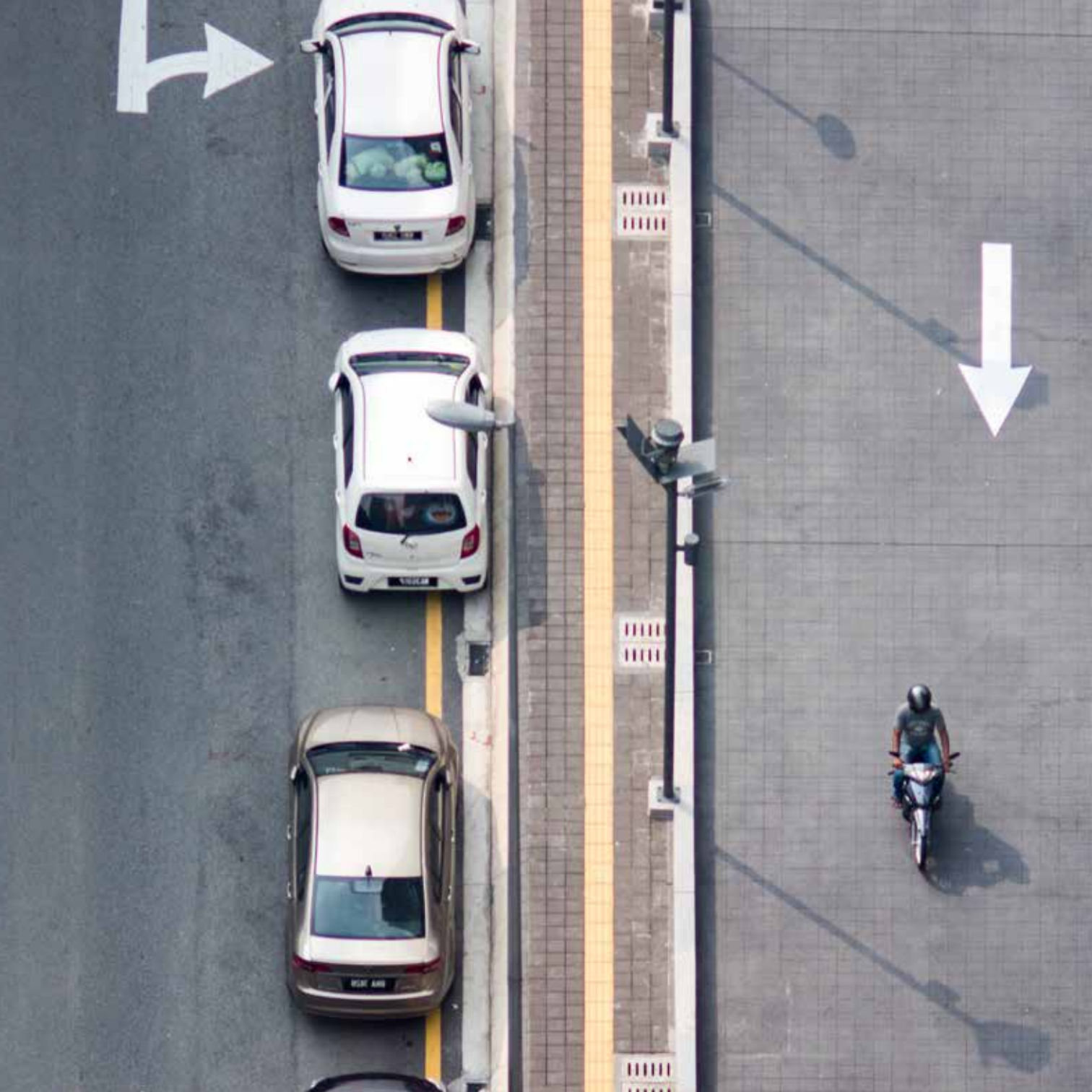
They provided training to all levels of employees, including senior management. They also republished the whistleblowing policy with a strong message, empowering employees to report issues. The policy emphasised that the company was serious about compliance, stressing the importance of everyone taking ownership to combat fraud together by speaking up.

As a result of their efforts, the company received a number of anonymous reports in the weeks that followed. These reports were taken seriously and some were passed to PwC fraud investigators for independent investigation.

The investigators contacted the whistleblowers and worked with them to learn more about their experiences. They assured the whistleblowers that they could maintain their anonymity. By collaborating with the whistleblowers, the PwC investigators were able to confirm and expose some serious issues in the company's sales and procurement functions. In some cases, the findings of the investigations resulted in referral to local law enforcement.

Some of the whistleblowers later contacted the head office via an anonymous email account to share their satisfaction with the response to their disclosures. They expressed appreciation for the way that the company took their concerns seriously and the fact that the company had engaged an independent party to investigate. By having a proper channel to speak up confidently, employees of all levels felt empowered to challenge unethical behaviours, and take ownership of the integrity of their respective teams.





Ensuring a fit-for-purpose compliance programme

So how does the C-Suite ensure that what they espouse is actually being put into practice? How is compliance being incentivised? How is it being measured?

Below are four key areas of focus for enhancing the effectiveness of ethics and compliance programmes. We examine these in the remainder of this section:



People and culture

Maintaining a values-based programme, measuring and rewarding desired behaviours.



High-risk areas

Better implementation and testing of the programme in high-risk markets and divisions.



Promoting accountability

Proactively managing the consequences of employee misbehaviour by communicating the implications of ethical lapses.



Technology

Better use of detection and prevention tools, including big data analytics.

Five steps to a more effective economic crime control programme





Technology: Not a cure, but a strong medicine

Today there are several sophisticated tools - including big data analytics capable of much more effective monitoring - that can help bring compliance closer to operations.

Yet outside of transaction-monitoring systems (which are used primarily by the finance sector), very few organisations are using these kinds of technologies to help detect and prevent economic crime. Globally, only 8% of respondents referred to the use of other internal monitoring approaches such as data analytics.

Helping our clients identify economic crime is just one of the ways we use data analytics. Data analytics can help us spot holes in controls and accounting procedures. These holes are the easily exploited opportunities that account for much of the economic crime in Malaysia.

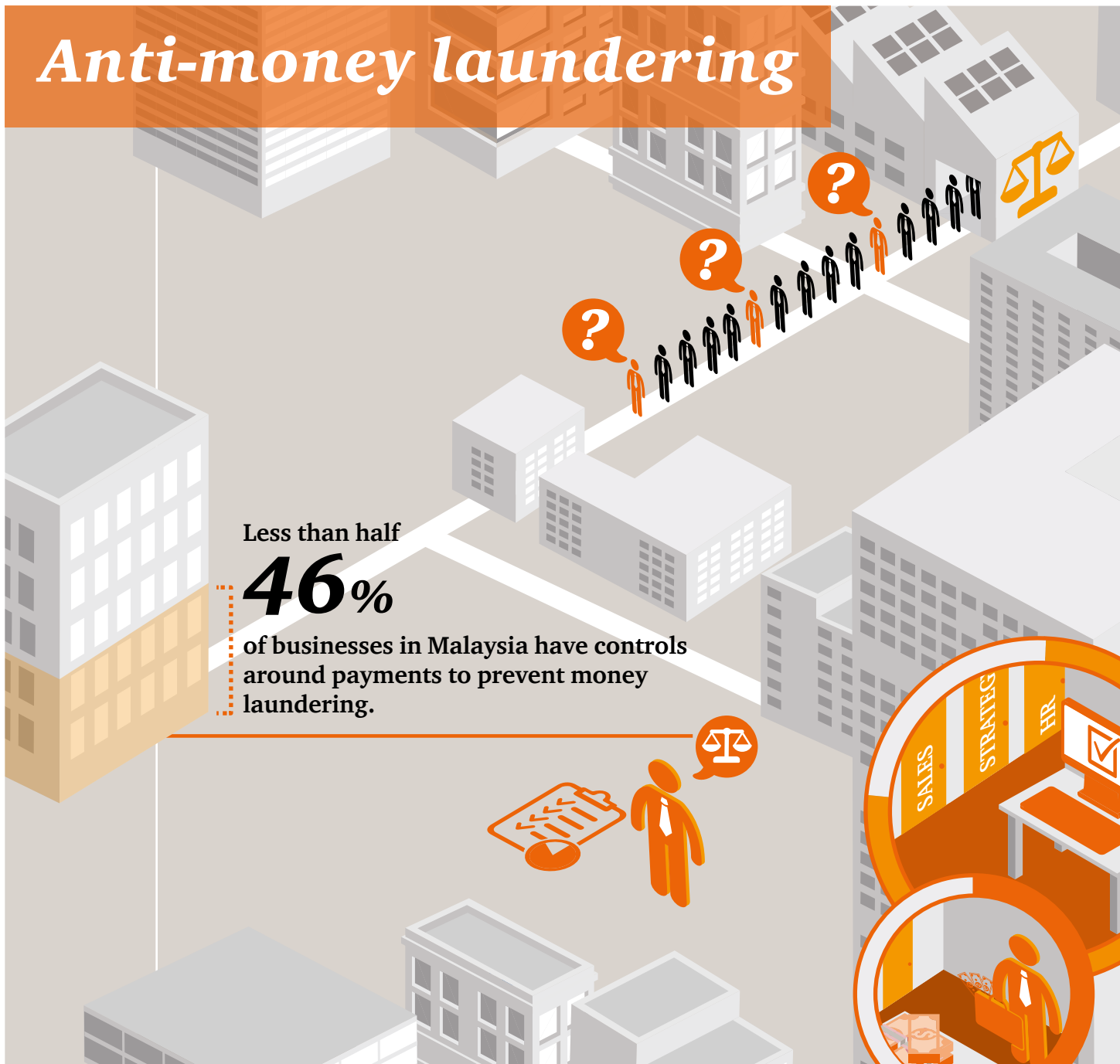
They can and should also be part of an organisation's control and monitoring. Having such controls in place at the time of the fraud can significantly limit the threat of damage.

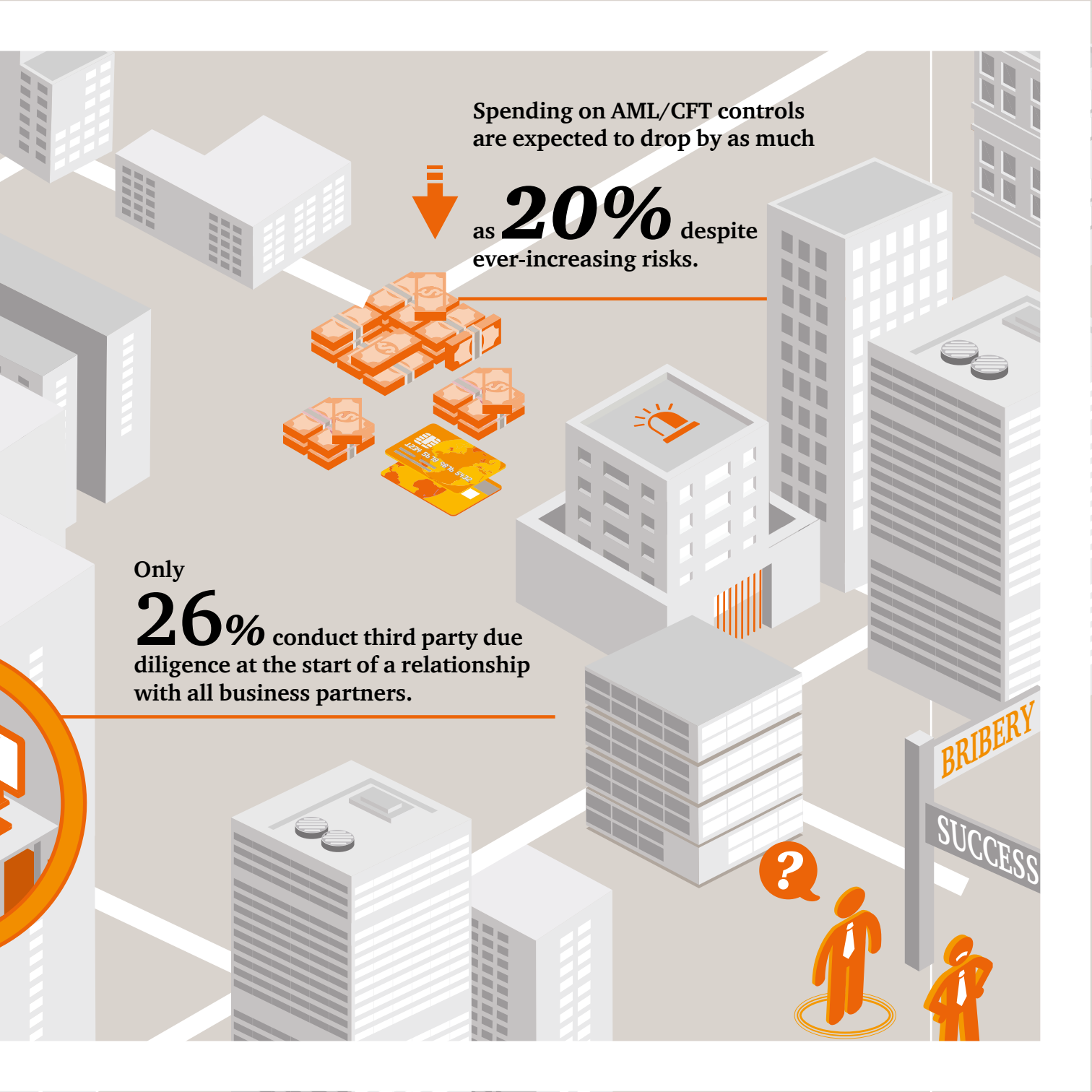
Anti-money laundering

Less than half

46%

of businesses in Malaysia have controls
around payments to prevent money
laundering.





Spending on AML/CFT controls
are expected to drop by as much

as **20%** despite
ever-increasing risks.

Only
26% conduct third party due
diligence at the start of a relationship
with all business partners.

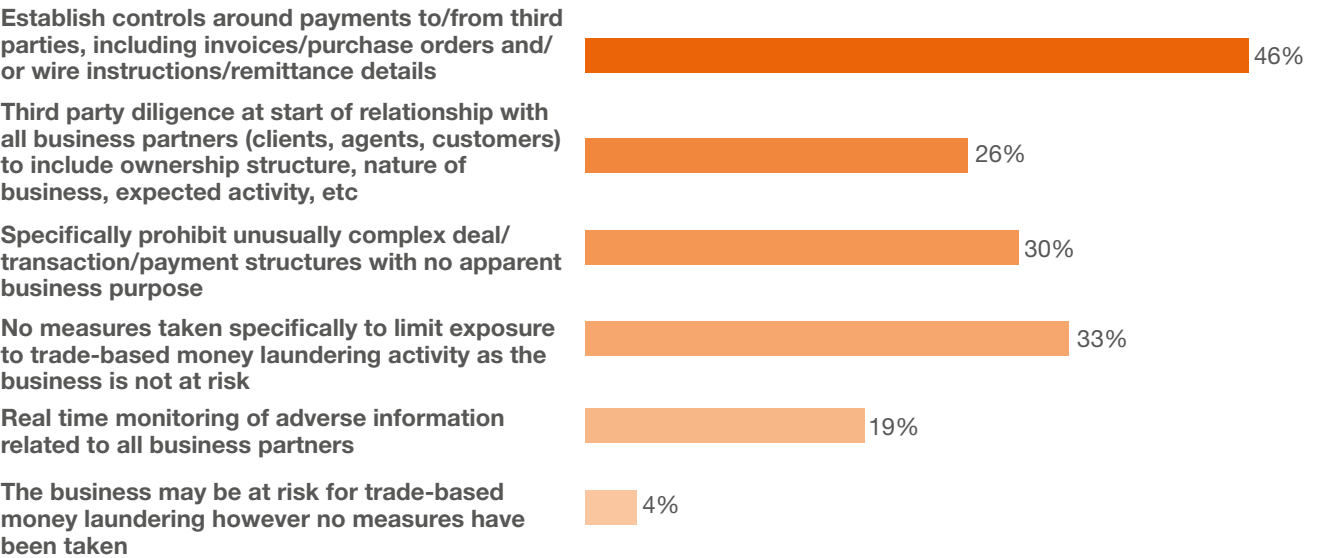
Anti-Money Laundering:

How will you respond to the fast-changing regulatory environment?

Money laundering is not just an issue for the financial services sector. For those organisations that become implicated, either deliberately or inadvertently, money laundering destroys value. It facilitates economic crime and activities such as corruption, terrorism, tax evasion, and drug and human trafficking, by holding or transferring the funds necessary to commit these crimes. It can be detrimental to an organisation’s reputation - and its bottom line.

In the chart below, Malaysian respondents indicated which measures they are taking to limit their exposure to trade-based money laundering and terrorist financing:

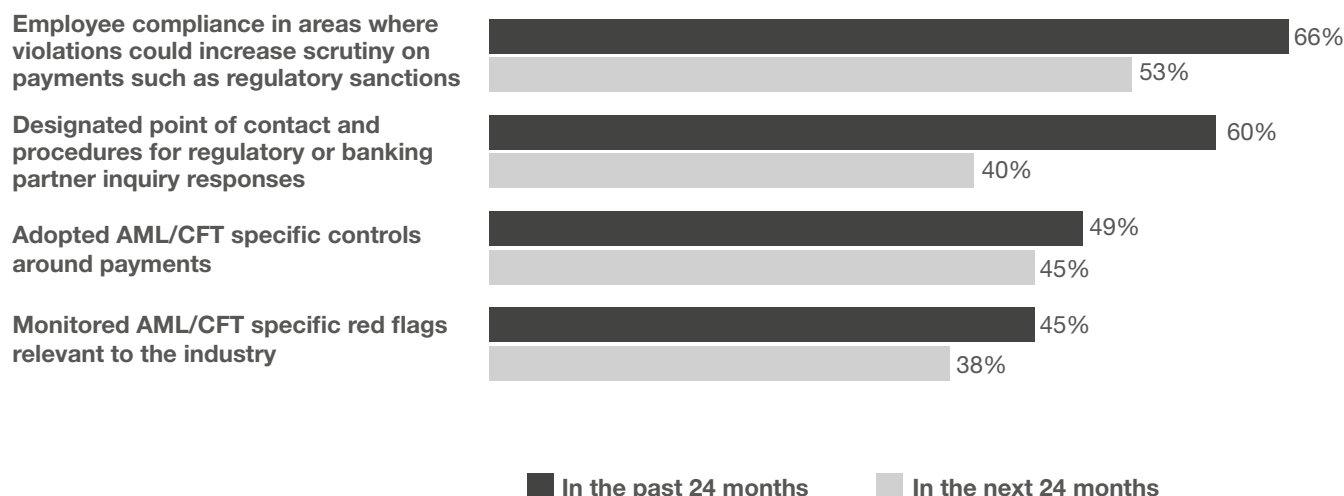
Fig. 8: Measures to limit exposure to trade-based money laundering and terrorist financing

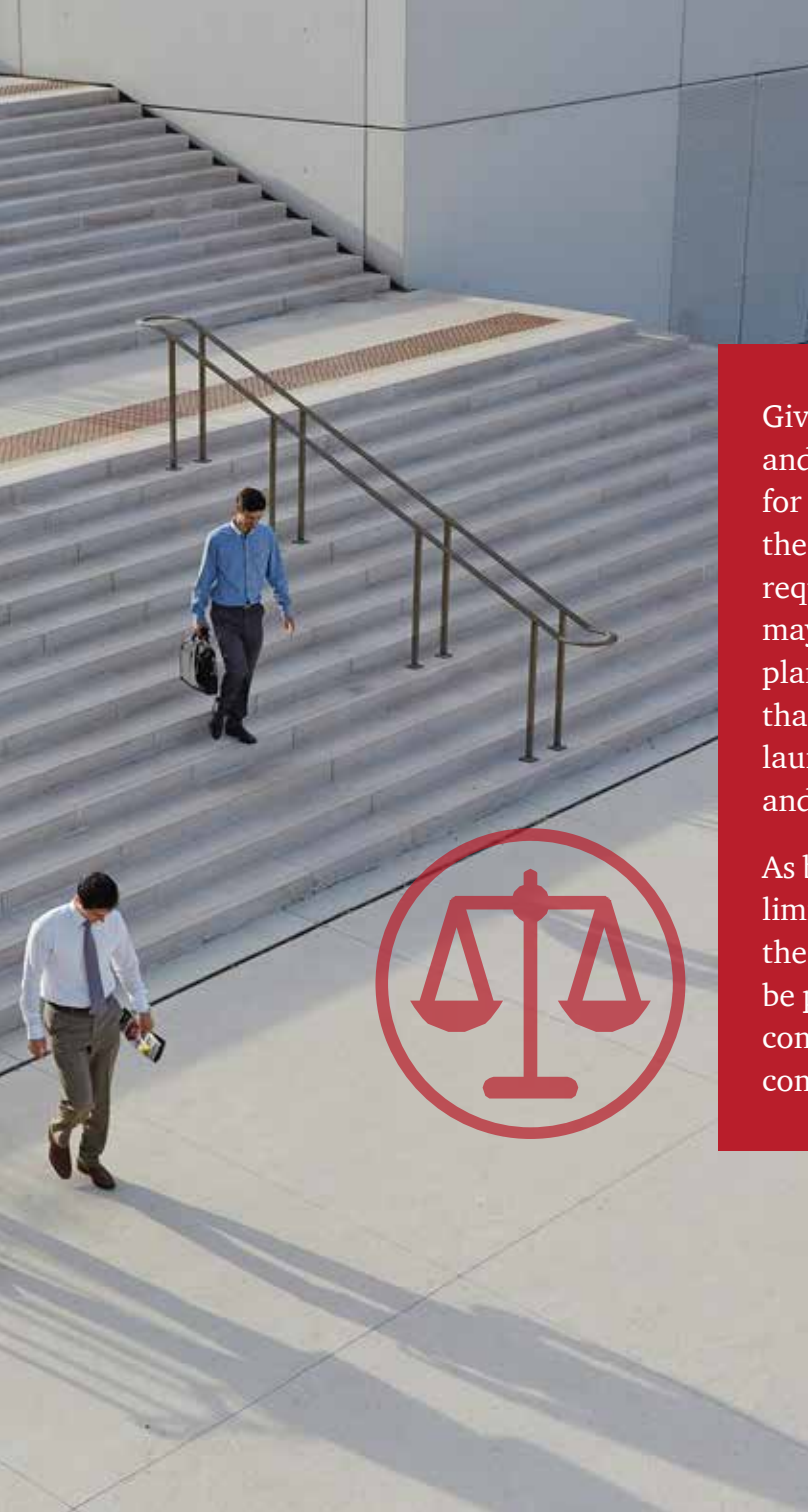


With less than half of organisations currently implementing controls around payments and only one in four conducting third party due diligence, we would expect to see companies planning measures to reduce exposure.

However, Malaysian companies appear to be reducing spending in all risk points of money laundering and terrorist financing. The chart below lays out the rate at which companies have spent in this area in the past two years, and their intended spending in the coming two years.

Fig. 9: *Spending to reduce exposure to money laundering and terrorist financing*





Given the rise of terrorism, money laundering and terrorist financing are a big concern for governments and organisations around the world. The increase in regulatory requirements can be onerous and costly. This may be the reason why some organisations plan to spend less in the coming two years than the two previous years on money laundering and terrorist financing prevention and detection.

As budgets are tightening and spending is limited, this may be no surprise. However, the risks continue and our region must be prepared to handle them. The costs of compliance may be high, but the costs of non-compliance are significantly higher.

What does this all mean for your company?

With the globalisation of anti-money laundering and countering the financing of terrorism (AML/CFT) standards, it's important to remember that especially for those in financial services, you may be judged by the highest international compliance standards. Here are two points to consider:

1) **Keep abreast of changing regulations**

To stay on top of regulatory changes, look beyond compliance with today's laws. Consider how upcoming regulations and trends affect your business.

2) **Think beyond geographical boundaries**

Since most transactions have a multinational financial component, it is good practice to default to the highest global standard of compliance whenever possible, and to undergo more rigorous AML/CFT self-assessments. Establish "enterprise-wide" requirements to ensure consistency across geographies.

Contacts



Alex Tan

Senior Executive Director and Forensics Lead

PwC Consulting Associates (M) Sdn Bhd

+60 (03) 2173 1338

alex.tan@my.pwc.com



Lim San Peen

Senior Executive Director and Business Recovery Lead

PricewaterhouseCoopers Advisory Services Sdn Bhd

+60 (03) 2173 1233

san.peen.lim@my.pwc.com



Pete Viksnins

Director

PwC Consulting Associates (M) Sdn Bhd

+60 (03) 2173 1406

pete.viksnins@my.pwc.com



Rohit Kumar

Director

PwC Consulting Associates (M) Sdn Bhd

+60 (03) 2173 1786

rohit.z.kumar@my.pwc.com

Participation statistics

In 2016, our respondents represented 17 industries. One-third of the respondents are publicly listed.

We are pleased to see a variety of functions of the respondents, with a healthy level of executive management taking part, as well as compliance and human resources staff.

There is also an even spread between top and middle management participation. Companies of all different sizes participated, from those with less than 100 employees to those with more than 10,000. The survey was conducted from 16 July-30 September 2015.

	% of respondents	
	2014	2016
Aerospace and Defence	0%	1%
Automotive	1%	1%
Chemicals	1%	0%
Communications	9%	1%
Energy, Utilities and Mining	11%	13%
Engineering and Construction	9%	6%
Entertainment and Media	4%	5%
Financial Services	19%	16%
Government/State Owned Enterprises	6%	18%
Hospitality and Leisure	1%	2%
Manufacturing	7%	12%
Insurance	10%	1%
Pharmaceuticals and Life Sciences	4%	0%
Professional Services	3%	8%
Retail and Consumer	11%	2%
Technology	0%	1%
Transportation and Logistics	0%	4%
Agriculture	0%	0%
Education	0%	1%
Healthcare	0%	0%
Other Industry/Business	0%	6%

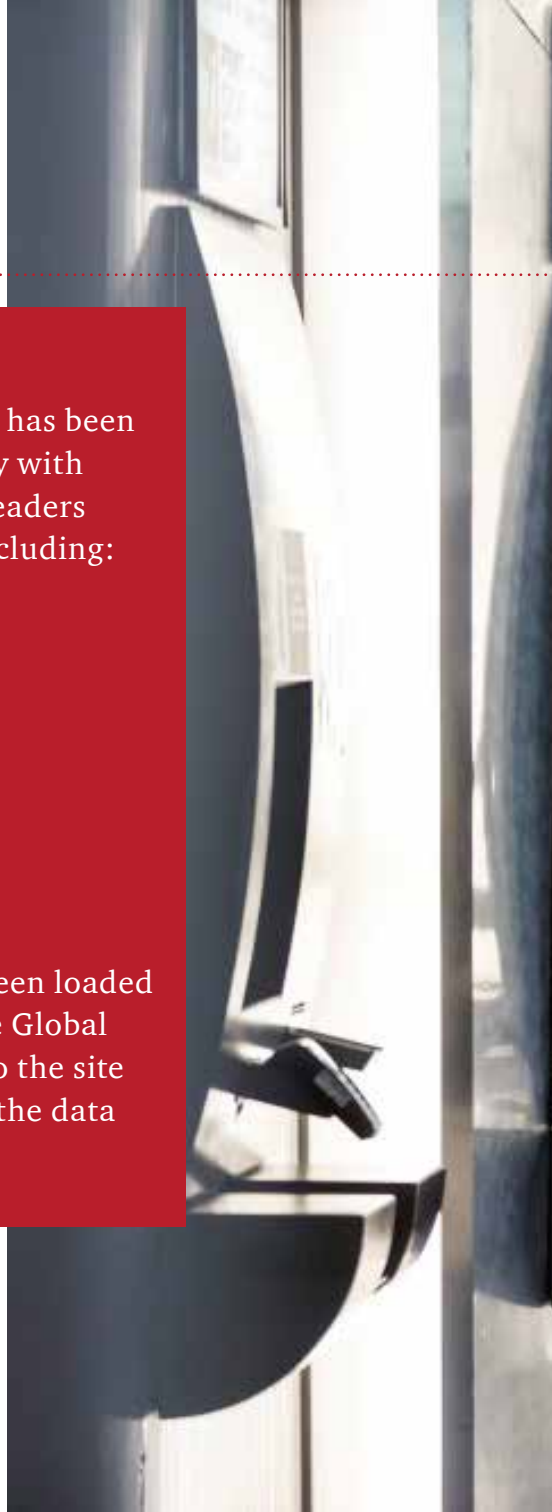
Data resources

Looking for more data?

The website www.pwc.com/crimesurvey has been designed to be an extension of the survey with many exciting and useful resources for readers wishing to delve deeper into the data, including:

- Survey methodology
- Terminology
- Comparative country counts
- Additional information regarding the nature of participants

In addition, this year's survey data has been loaded onto an innovative tool referred to as the Global Data Explorer which will allow visitors to the site the ability to customise their analysis of the data for their specific needs.





NEXT TIME BUY YOUR MOVIE
TICKETS ONLINE AT CINEPLEX.COM
PRINT
SKIP
SCAN

NEXT TIME BUY YOUR MOVIE
TICKETS ONLINE AT CINEPLEX.COM
PRINT
SKIP
SCAN

NEXT TIME BUY YOUR MOVIE
TICKETS ONLINE AT CINEPLEX.COM
PRINT
SKIP
SCAN

NEXT TIME BUY YOUR MOVIE
TICKETS ONLINE AT CINEPLEX.COM
PRINT
SKIP
SCAN

CINEPLEX
TICKETING

CINEPLEX
TICKETING

CINEPLEX
TICKETING

www.pwc.com/crimesurvey

© 2016 PwC Consulting Services (M) Sdn Bhd. All rights reserved. "PricewaterhouseCoopers" and/or "PwC" refers to the individual members of the PricewaterhouseCoopers organisation in Malaysia, each of which is a separate and independent legal entity. Please see www.pwc.com/structure for further details. CS08511