PwC's Global Economic Crime and Fraud Survey 2018

Southeast Asia Report

pwc

www.pwc.com

Foreword

PwC's purpose, to build trust in society and solve important problems, resonates with me as I read the results from our survey and this report. Fraud and economic crime have been growing in both occurrence and in publicity in recent years across Southeast Asia. This matters to everyone. Southeast Asia is fundamentally linked to supply chains around the world. PwC's recent publication *"The Future of ASEAN - Time to Act"* shows that the region continues to move strongly on the growth path. Its GDP is projected to touch US$4 trillion by 2022, when it is forecast to become the fifth-largest economy worldwide. The region also plays an important role on the global political stage and is no longer just an importer of business, culture and ideas but an exporter too. The rise of fraud and economic crime in such an important region is enough to make businesses, politicians and society as a whole sit up and take notice.

This worrying trend should be seen in the context of the five broad 'Megatrends' PwC has identified that will shape the region and the world for years to come:

- Rapid urbanisation;
- Climate change and resource scarcity;
- Shift in global economic power;
- Demographic and social change; and,
- Technological breakthroughs.

First, ***rapid urbanisation*** can be seen from Manila to Jakarta, from Kuala Lumpur to Yangon. As populations become more concentrated, organisations benefit more from economies of scale and have access to broader bases to sell to or serve. This concentration and growth fuels all aspects of the economy - including the criminal and fraudulent.

Second, ***climate change and resource scarcity*** is going to continue mounting pressure on governments and societies as we try to do more, for larger populations, with less. Pressures and incentives to perform to expected standards are common drivers of fraud. By definition climate change and resource scarcity are going to be increasing these pressures - and there is a risk that these pressures will force unethical behaviour in response.

Third, the ***shift in global economic power*** places the wider Asia-Pacific at the heart of international focus. The Southeast Asian region is seizing the opportunity to benefit from this focus and to take the limelight. With the world's attention on us growing, our society and our organisations must hold each other to account and shine a light on fraud and economic crime.

Fourth, ***demographic and social change*** is putting never-before-seen levels of pressure on our healthcare and public services, and on what societies expect of their governments. As mentioned above, increased pressure often leads to increased instances of fraud. Additionally, sweeping and fundamental changes can come with uncertainty and potentially poorly understood new norms. Inadequately managed change and uncertainty carry greatly increased risks of fraud.

Fifth, and arguably the Megatrend with the impact that's most difficult to predict, is ***technological breakthroughs***. From quantum computing to CRISPR/Cas9 gene editing, from leaps in artificial intelligence to the Internet of Things, the pace of technological advancement can sometimes be breathtaking. The potential benefits of such change are broad and far reaching, but it's important to remember that just as you or I can benefit from technology, so too can criminals and fraudsters.

Alongside these Megatrends, and more specific to our region, are the ever increasing regulatory pressures businesses across Southeast Asia are facing. From major anti-corruption drives to strengthening anti-money laundering regimes, governments in every country are responding to public demand and stepping up their expectations. It is vital that businesses both understand these challenges, and adapt to overcome them.

With all this in mind, building trust and solving the problems that matter really need to be high on anyone's agenda. I welcome you to read this report and to join us in the conversation about fraud and economic crime.

Sundara Raj Ramamurthy
Partner
CEO and Markets Leader, PwC Southeast Asia Consulting

Preface

PwC has run the Global Economic Crime Survey for over a decade and a half. Drawing on responses from more than 7,200 organisations in every industry from around the globe, including 1,012 from Southeast Asia, this year's survey helps to bring fraud out of the shadows by shining a light on what has been called 'the largest competitor you didn't know you had'.

2018 marks the first year we have launched a Southeast Asia report. Covering Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam, our report speaks to the growing importance of the region, and the hand-in-hand growth of fraud and economic crime.

The data this year show a fairly significant rise in fraud and economic crime. 46% of Southeast Asian respondents reported experiencing such in the past two years. This contrasts with the 2016 and 2014 figures of 26% and 28% respectively. Our report delves a little into what the drivers of this change might be, but I like to think that this rise is not indicative of a wider deteriorating state of affairs. Rather, organisations are becoming more alert to the threat that fraud and economic crime represent.

I would like to highlight the three key themes that our Southeast Asia survey data have revealed. First, strong hierarchical cultures and clearly defined chains of command, that in extremes can result in a lack of empowerment for the people of an organisation. Second, the power of relationships. Southeast Asian businesses, more so than in many other parts of the world, place tremendous value on the strength of their professional relationships. These networks can lead to mutually beneficial and sustained growth, but they can also create blind spots and lead to conflicts of interest if not properly managed.

Third, the importance placed on tradition. Although the value of protecting one's culture and how things have always been done successfully should not be understated, taking it too far can lead to a resistance to change. These themes reflect some of the core elements of doing business in the region, providing some of Southeast Asian businesses their greatest strengths and, as the data show, their greatest weaknesses.

Should you be interested in delving deeper into the data, please don't hesitate to reach out to either myself or your local PwC contact for our territory-specific reports, or to discuss how our findings might impact you, your business, and your society.

Richard Major
Partner
Forensic Services Leader, PwC Southeast Asia

Contents

Key Findings

In the last two years, out of 1,012 respondents in Southeast Asia*

46%
experienced fraud and economic crime, up from
26% in 2016

66%
of fraud and economic crime was committed by internal members of staff

12%
have not performed any kind of economic crime-related risk assessment

21%
detected and reported cybercrime, lower than the global average of
31%

10%
leveraged AI or Advanced Analytics to counter fraud

77%
reported that they either don't know of any plans or have no plans to use AI or Advanced Analytics

39%
experienced business conduct/ misconduct and

27%
experienced procurement fraud

34%
had performed a cyber-attack vulnerability risk assessment

39%
reported that they either don't know whether they have a Cyber Security programme, or confirmed they don't have one

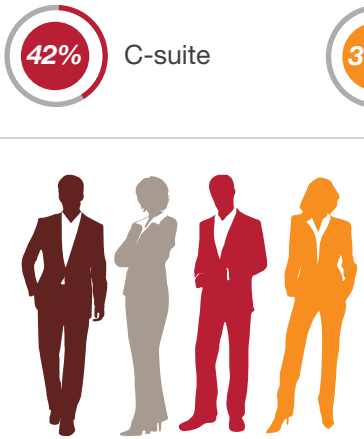
43%
of frauds were proactively detected through corporate controls

32%
of frauds were reactively detected through corporate culture

*Singapore, Malaysia, Thailand, Vietnam, Indonesia and the Philippines

About the survey

The 2018 survey questionnaire was open to participating organisations in late 2017. There were 1,012 respondents from Southeast Asia representing 14% of all global respondents.



42% C-suite

31% Department heads

27% Managers/other

52% worked for multinational companies

56% worked for organisations that employ over 1,000 people, **almost half** of whom worked for organisations with more than 10,000 employees

50% represent publicly traded companies

Top Industries

22% Manufacturing

20% Financial Services

6% Energy, utilities and mining

5% Automotive

5% Insurance

A typical Southeast Asian respondent to our survey is a member of senior or upper management working at a medium-to-large company that operates in multiple countries around the world. If they don't work in executive management (26% of respondents), they are part of finance (17%), audit (14%) or risk management (6%). Globally, respondents tended to be more from finance (22%) than executive management (18%) or audit (12%), however the seniority of respondents is similar to that of respondents from Southeast Asia.

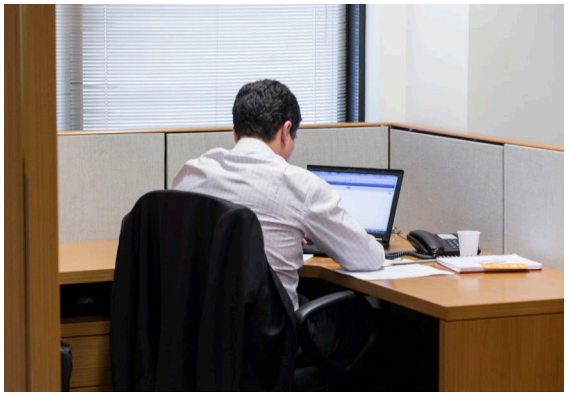
The organisations that global respondents work for are more multinational (60% compared with 52% regionally), with similar-sized operations (55% employ more than 1,000 people). Global respondents are more evenly spread across industries, although financial services (FS) and manufacturing are still the best represented industries (22% and 11% respectively globally).

Southeast Asia is comprised of a rich diversity of economies, from the developing agrarian/ industrial countries, to the advanced services economies, and everything in between. We ask the reader to keep this in mind when considering the results.

We have tried to provide as granular detail as possible. Where the data was insufficient, we have aggregated responses to ensure statistical validity. We have excluded Myanmar in our country breakdowns for this reason.

Fraud and economic crime - past and future

Fraud and economic crime - underreported and underestimated

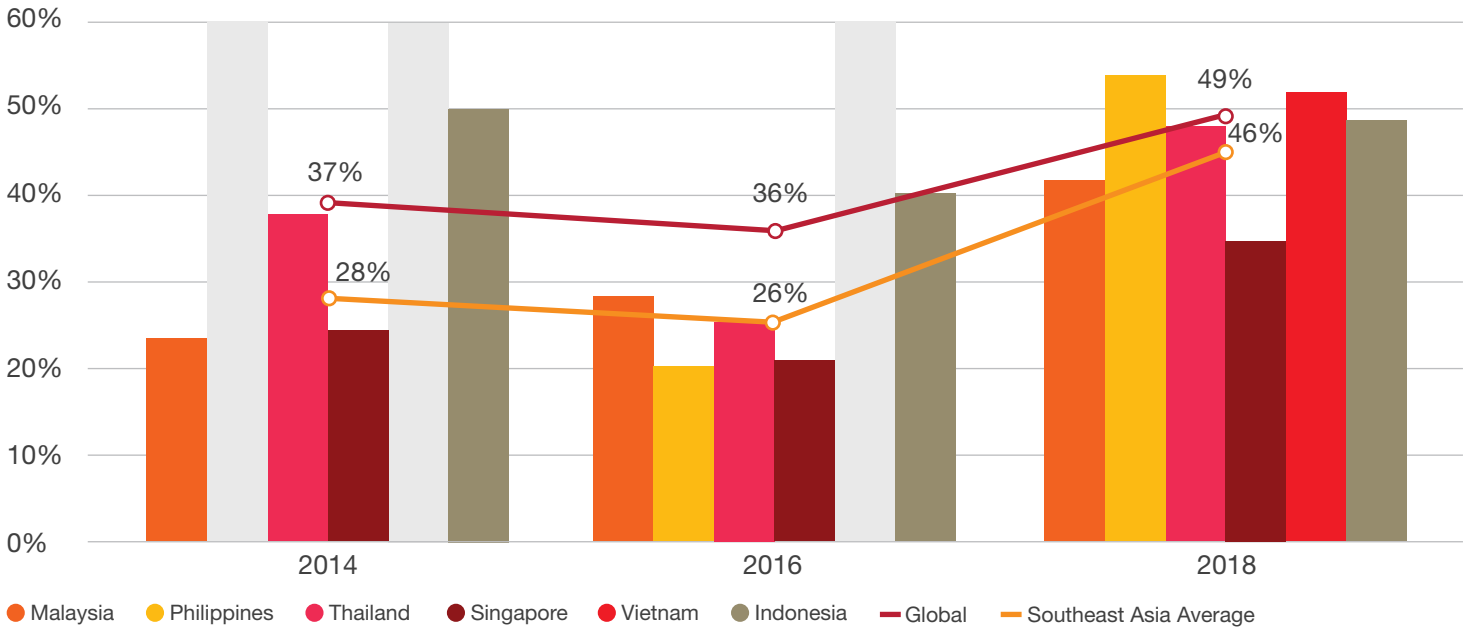


Fraud and economic crime are on the rise across Southeast Asia. 46% of respondents reported being the victim of fraud or economic crime in the past 24 months. This is reflective of a slightly better position than the global average (49%), but represents a significant jump on prior years (26% in 2016 and 28% in 2014).

Drilling deeper into the data, Singapore and Malaysia reported more favourable experiences than the regional average (35% and 41% respectively). The Philippines appears to have suffered the most over the last two years, with over half (54%) of respondents reporting fraud and economic crime.

These increases can in part be attributed to a greater awareness of economic crime, suggesting that fraud detection methods are at least gradually improving.

Has your organisation experienced fraud or economic crime in the past 24 months?



46% may sound like a lot. In fact, the reality is likely to be much higher. In our experience, the majority of frauds go undetected. Various factors have contributed to the underreporting of fraud and economic crime, but fear of embarrassment may be one of the most prominent reasons.

In Southeast Asia, many employers will quietly investigate and resolve instances of fraud internally to minimise their risk of, and exposure to adverse publicity. This, alongside with the fear of damage to relationships, has brought the reported figures down. The real statistics likely paint a far darker picture.

Note:

Data for Philippines in 2014 is not available;
Data for Vietnam in 2014 and 2016 are not available

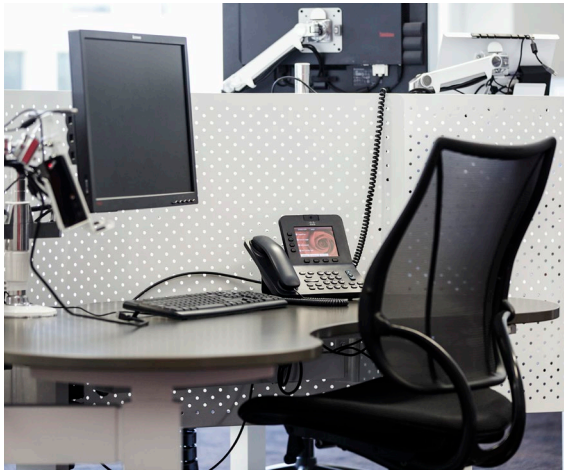
The flavours of fraud and economic crime

Of the fraud and economic crime reported by Southeast Asian respondents, asset misappropriation continues to be the most common (52%). This is above the global average of 45%.

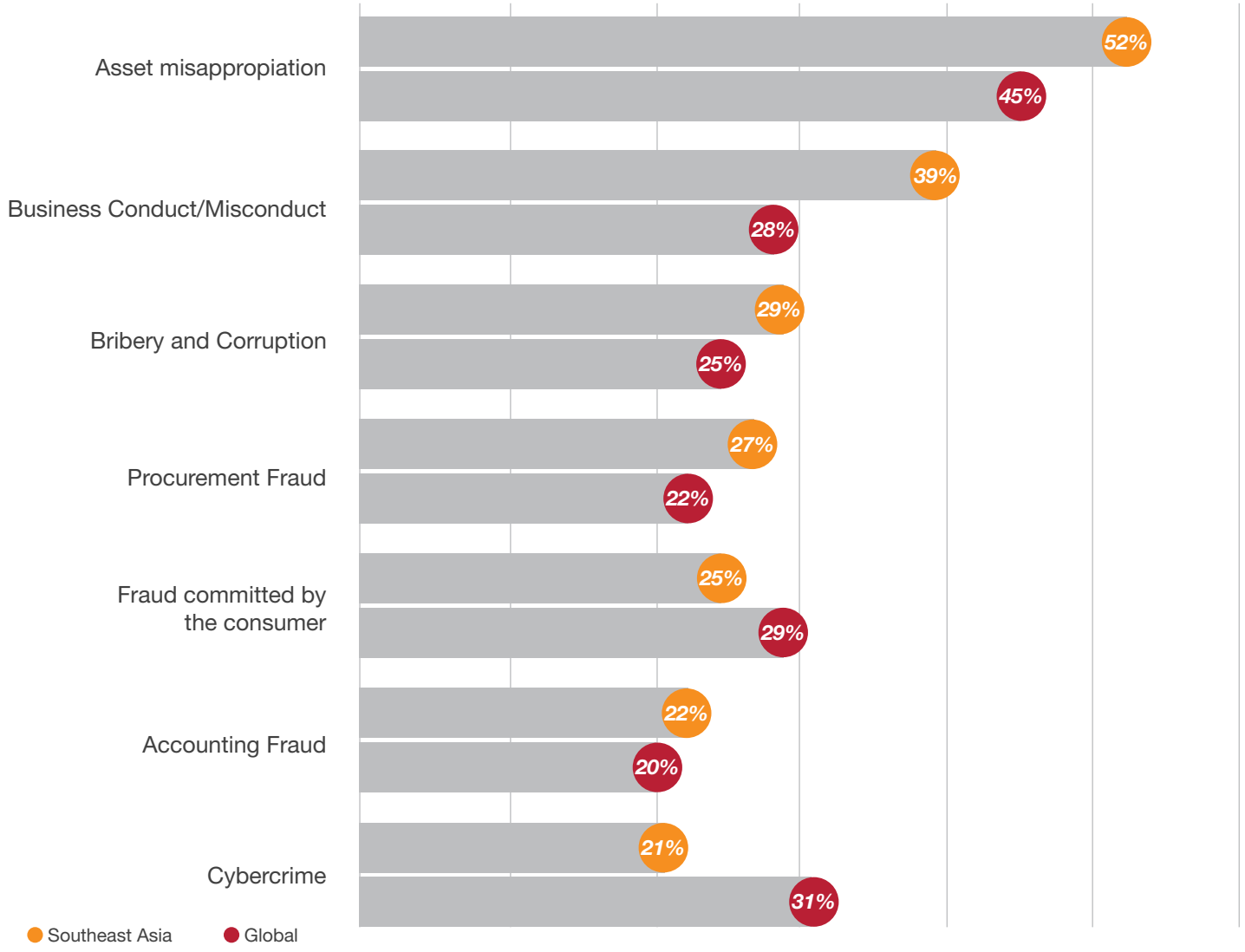
Aside from asset misappropriation, the most reported 'flavours' of fraud are business conduct/ misconduct (39%), bribery and corruption (29%), procurement fraud (27%), and fraud committed by the consumer (25%).

A new category this year, business conduct/ misconduct is defined as "frauds or deception by companies upon the market or general public". For example, in the absence of strong regulators and weaker customer protection laws, companies in Southeast Asia may in the past have gotten away with exaggerated marketing claims or even false marketing.

Regardless of the flavour, fraud and economic crime leave a bitter taste for all who fall victim.



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



The Southeast Asian secret recipe

If not properly managed, the very strengths that set Southeast Asian businesses apart are the ingredients in a secret recipe that can create opportunities for fraud and economic crime. A business partnership based on close relationships is naturally a strong one. But in some instances those relationships can be cemented illegally.

29% of Southeast Asian respondents have reported instances of bribery and corruption.

Interestingly, and perhaps through a desire to protect those very relationships, only ***23% of respondents reported*** being asked to pay a bribe.

Business relationships that verge on the inappropriate are not the only factor contributing to fraud and economic crime in the region. The culture of strong hierarchies has led to well managed and disciplined firms competing on the global stage. However, it has also prevented many from questioning their superiors or raising concerns when they see something wrong. 54% of internal fraud was perpetrated by senior or middle management, and 29% by junior management. This is a concerning shift from 2016 responses, when the figures were 38% and 47% respectively. We ponder how the statistics might change if there was a culture of speaking up against unethical business practices.

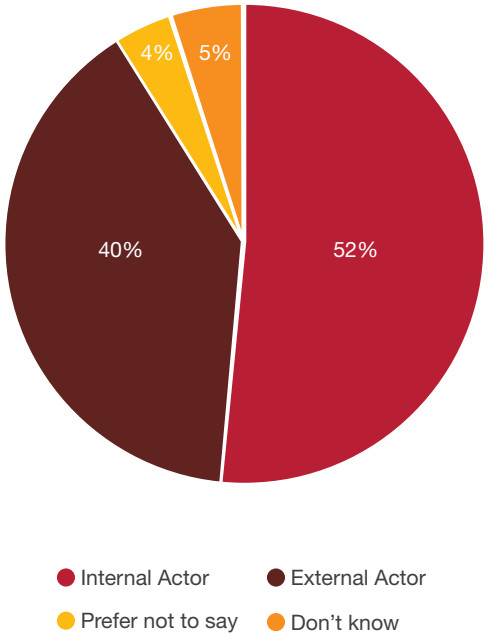
A strong hierarchical culture can be linked to a selective resistance to change. Change can be the next best thing, or it can cause unnecessary disruption. Having a "I've done this longer than you" or "Why now?" mentality as a defensive reaction to unwanted suggestions can harm a company's ability to fight fraud and economic crime. This risk is particularly acute given the constant evolution of new technologies that could help to fight fraud and economic crime (see pages 28-29). Management may be too familiar with their old routines, or they could fear changes that they perceive might diminish their power.

The c(r)ooks in your restaurant

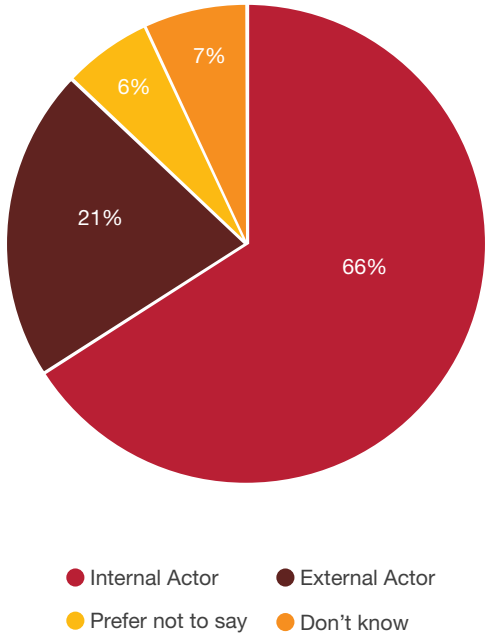
Southeast Asia follows the global trend of internal actors being the main perpetrators of fraud and economic crime. However, in Southeast Asia, it is much more likely that any given culprit works for the victim organisation (66% versus the global average of 52%). Consistently across all surveyed Southeast Asian countries, culprits are more likely to be the employees of the company – the enemy within.

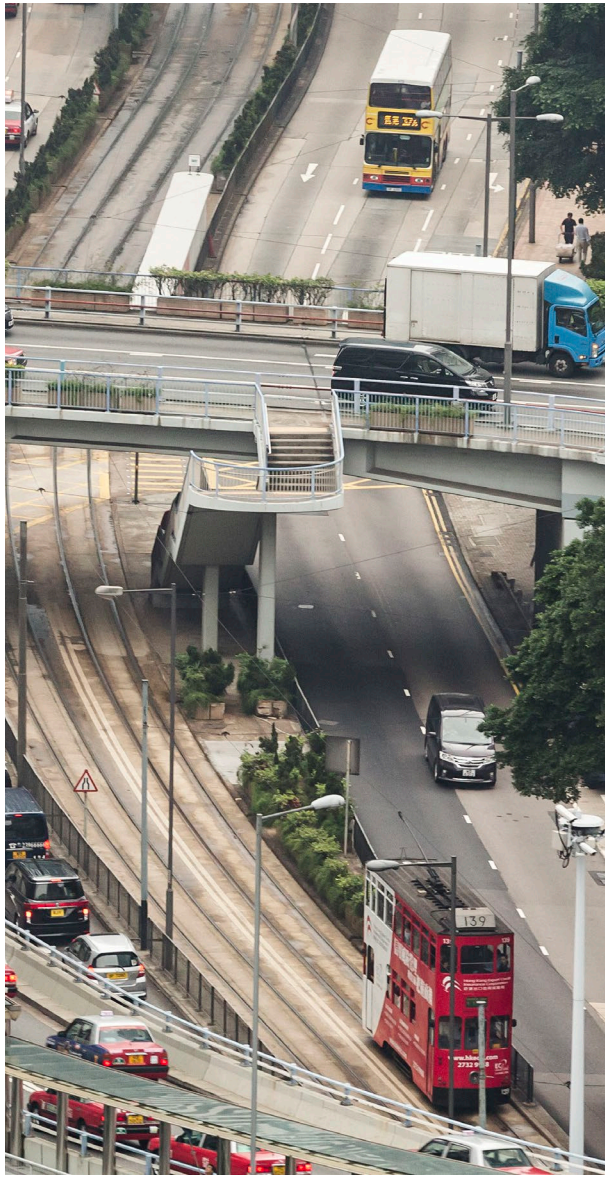
The high level of internal actor-driven frauds could also be a reason why asset misappropriation, business conduct/ misconduct, bribery/corruption and procurement fraud (four of the five most encountered frauds) are high. These types of crimes often require the involvement of internal actors.

Who was the perpetrator of the most disruptive fraud in the last 24 months? - Global



Who was the perpetrator of the most disruptive fraud in the last 24 months? - Southeast Asia





The c(r)ooks in your restaurant

Of the internal perpetrators of fraud and economic crime, 19% were senior management, 35% middle management, 29% junior management and 13% other members of staff.[1] Although these staff come from all areas of their companies, three departments stand out: marketing and sales (19%); operations and production (18%); and procurement (14%).

The senior and middle management band of respondents represent the majority of internal actor driven fraud (54% in total). Given the culture of hierarchy commonly seen in Southeast Asian businesses, this is a cause for concern as management are often in a unique position to commit fraud. The ability to override controls combined with an intimate knowledge of how those controls and the wider business functions provides management with the ***opportunity*** to commit fraud.

The high performance culture that goes hand in hand with rapidly growing economies and strong hierarchies can, in the wrong situations, lead to unreasonable ***pressures*** or even ***incentives*** to commit fraud. The personal justification of dishonest actions is the final element needed to precipitate fraud. The ***rationalisation*** of one's actions, in the form of 'I deserve this', or 'I'm just borrowing it', or even 'I want to hurt my company', can come from anywhere. However, it is often reinforced in organisations where staff and junior management see, or think they see, their superiors acting dishonestly. As the saying goes, "the fish rots from the head".

Who is the main perpetrator of the most costly internal fraud?

Senior Management

Middle Management

Junior Management

In which function does the main perpetrator of the most costly internal fraud reside?

Marketing and Sales

Operations and Production

Procurement

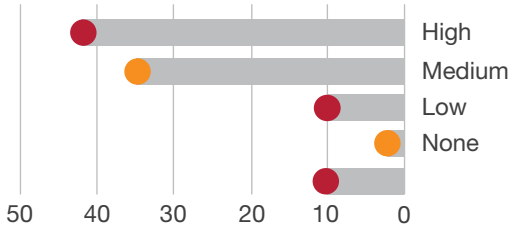
[1]3% of respondents did not identify the main perpetrator

The c(r)ooks in your restaurant

These three elements, ***opportunity, pressure/ incentive,*** and ***rationalisation,*** come together to create the 'perfect storm' of fraud that is illustrated by the fraud triangle. It is interesting to note that respondents in Southeast Asia ranked the three fraud-enabling elements' relative importance the same as the global average rankings.

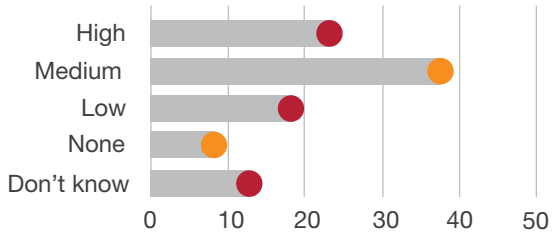
The most significant ingredient, opportunity (78%) is encouragingly matched by the highest level of investment in the corresponding response-business processes. Worryingly, the corresponding level of effort cannot be seen in promoting ethical decision making or in addressing organisational or structural influencers of fraud.

What level of effort do you put into business processes to limit opportunities to commit fraud?

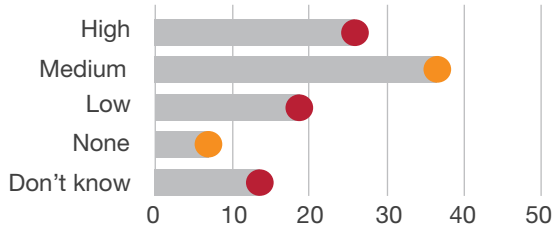


The Fraud Triangle

What level of effort do you put into encouraging ethical decision making?



What level of effort do you put into addressing organisational and external incentives or pressures to commit fraud?

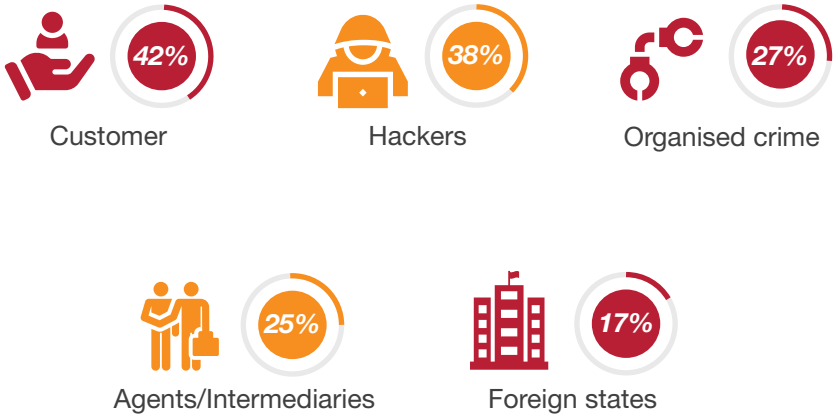


The travelling chefs

External actors, on the other hand, represent 21% of reported frauds, with customers being the most significant culprit (42%), followed closely by hackers (38%), organised crime (27%) and agents/ intermediaries (25%). Concerningly, 17% of the main perpetrators of external fraud were foreign states. Although speculative, this could indicate a prevalence of industrial and commercial espionage in Southeast Asia.

Despite the fact that external actors are responsible for a minority of frauds, they present a very real threat. These parties can be a significant blind spot for organisations, after agents, vendors or shared service providers have been invited to do business with them. It's only natural for organisations to expect a certain degree of mutual trust in these relationships, but this trust can sometimes be misplaced.

Who were the main perpetrators of external fraud against your organisation?

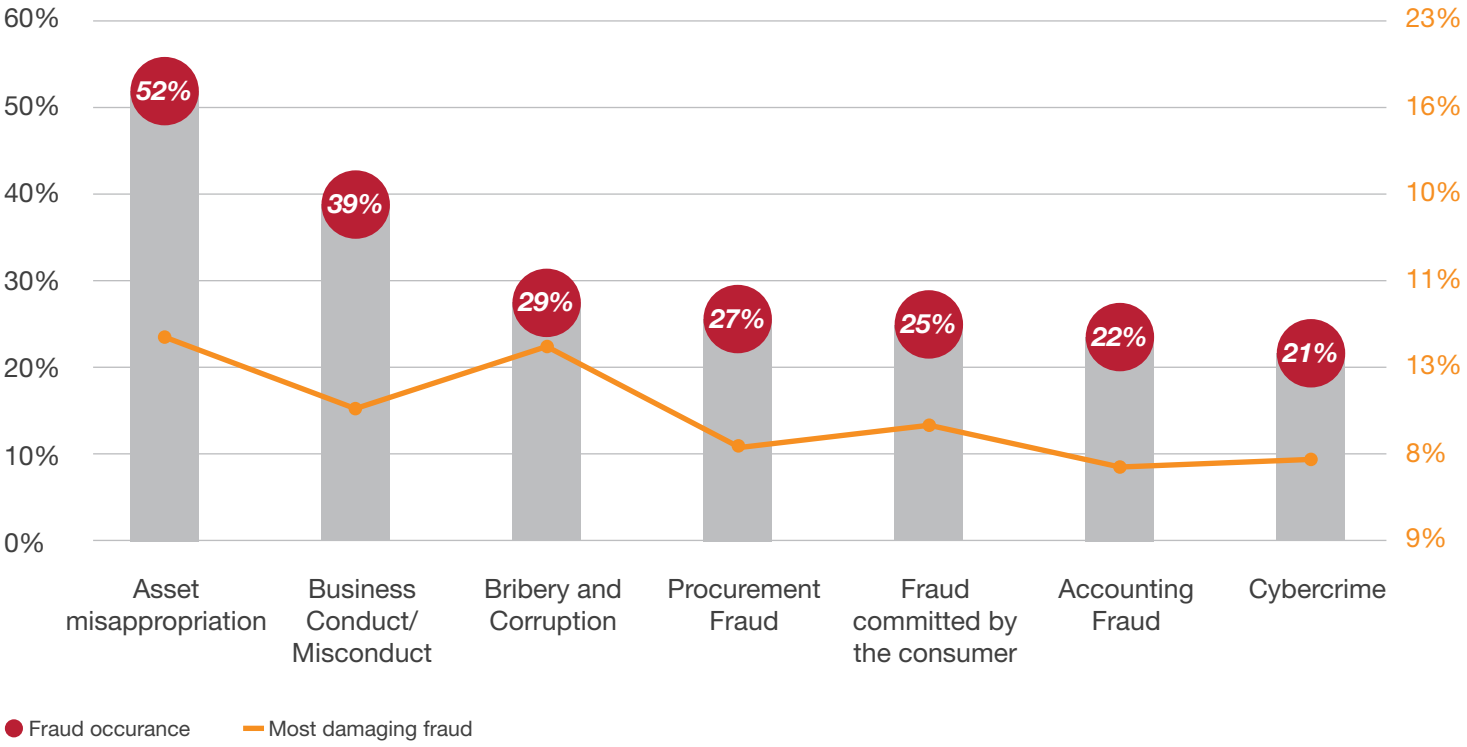


Financial losses and morality - the big casualties

When comparing the most damaging fraud with the most common in Southeast Asia, unfortunately the more prevalent flavours of fraud were also the more costly ones.

In Southeast Asia, 15% of respondents reported more than USD 1 million in losses. This is in line with the global trend, where 19% of respondents claimed losses were more than USD 1 million.

What types of fraud and/ or economic crime has your organisation experienced within the last two years, and which were the most financially damaging ones?

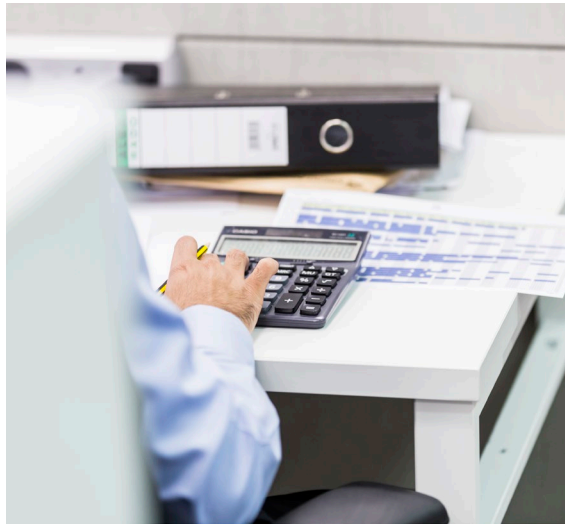


More than just the surface

Aside from direct financial losses, there are often indirect financial costs associated with fraud, such as:

- Productivity losses
- Unnecessary expenses
- Costs of response

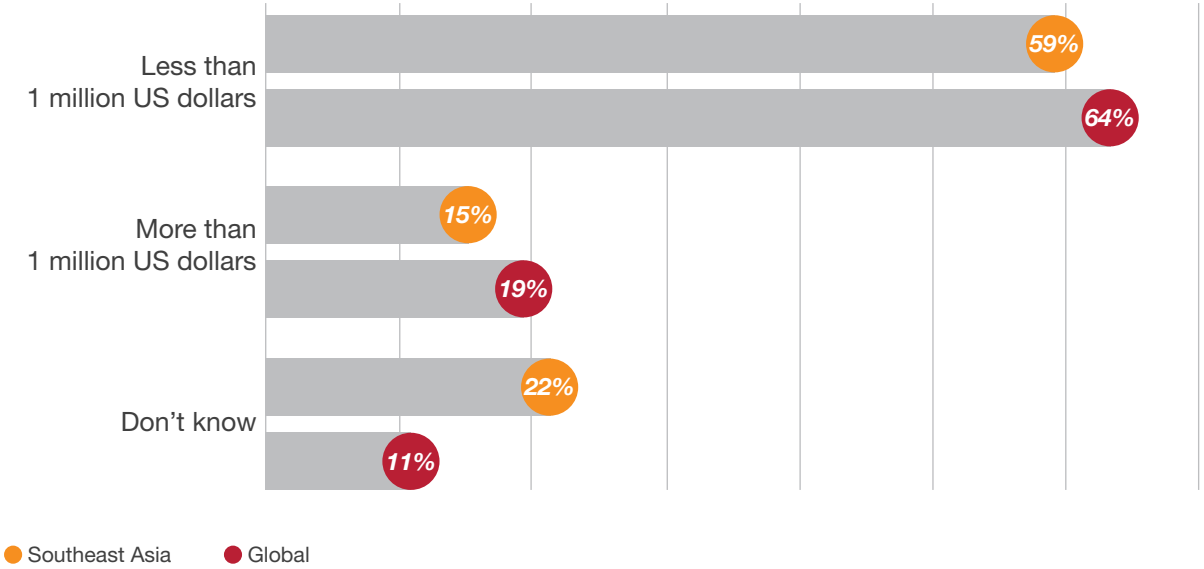
As time goes by, new forms of indirect costs appear. For example, the Indonesian government now includes environmental damages in the calculation of the impact of corruption in quantifying fines.



Financial losses and morality - the big casualties

Concerningly, 22% of Southeast Asian respondents (11% globally) indicated that they did not know how much their organisation may have lost through fraud. Unsurprisingly, when asked whether the amount spent by their organisation on responding to crime was more, less or equal to that lost through such crime, they were unable to tell us. Whether ignorance or a lack of transparency is the cause, neither reason is encouraging. It's worth noting that all these respondents were managers and above in their organisations, so would be expected to know this information.

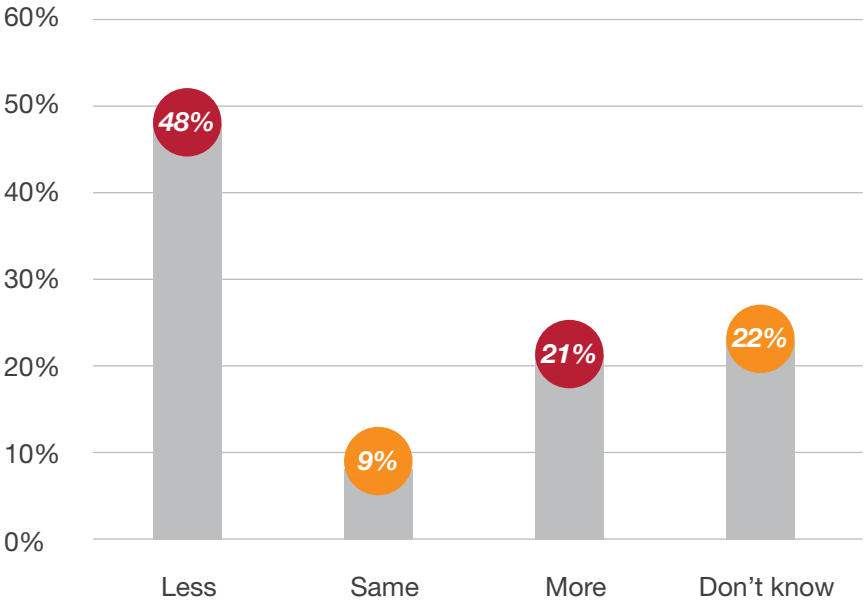
In financial terms, approximately, how much do you think your organisation may have directly lost through the most disruptive crime over the last two years?



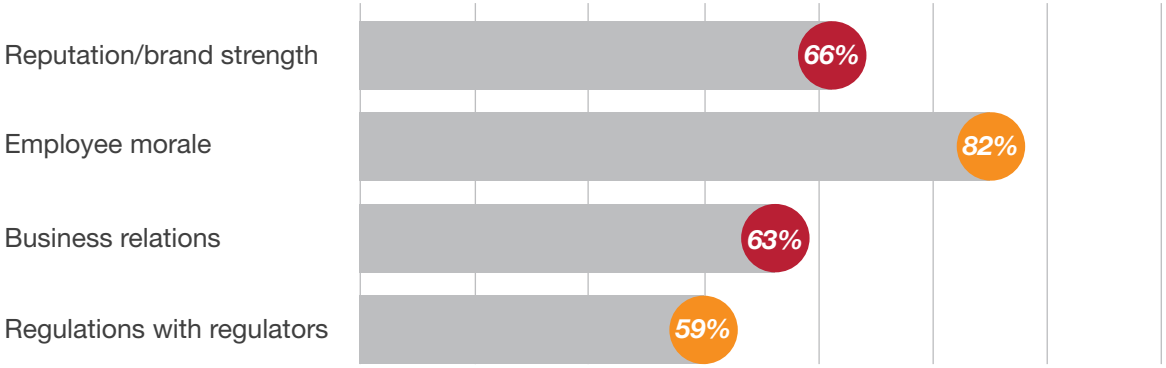
Salt to the wound

As if the financial cost of fraud and economic crime were not enough, 82% of respondents reported employee morale being negatively affected by instances of fraud. This is perhaps not surprising. More than half of all respondents have reported damage to their reputation or brand strength, business relations, and relations with regulators. These results are similar to the global responses. Additionally, these 'soft' damages further exacerbate financial losses, as they can lead to a loss of business, loss of productivity and broken trust and relationships.

As a result of the most disruptive crime experienced in the last two years, was the amount spent by your organisation on investigations and/or other interventions, more, less or the same as that which was lost through this crime?



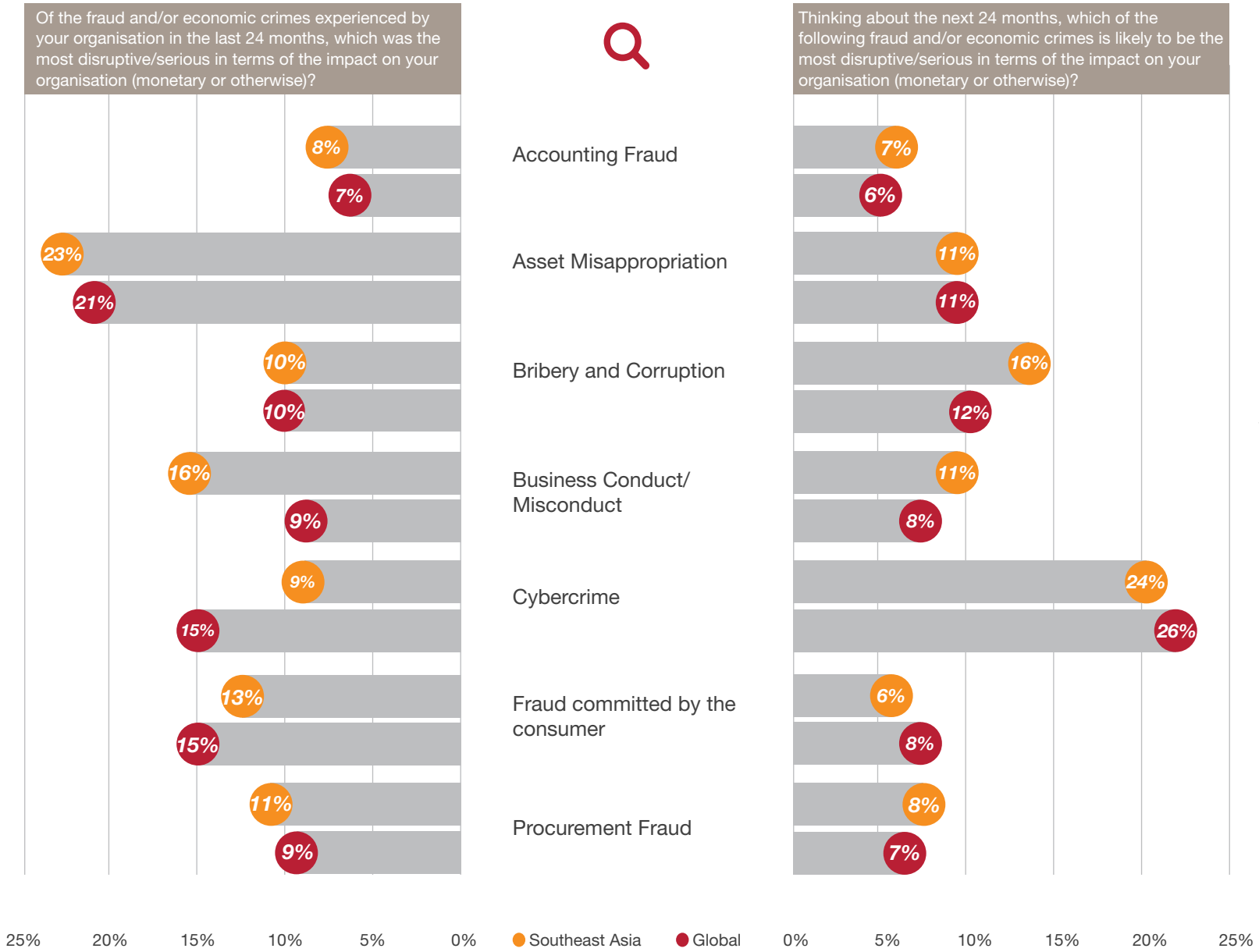
What was the level of impact of the most disruptive crime experienced on the following aspects of your business operations?



Organisations should spend money to counter fraud and limit financial and other losses, but this expenditure doesn't have to break the bank. Close to half of respondents have found that the cost of fraud prevention is less than the direct losses from the crime itself. Only around 21% of respondents had indicated that fraud prevention is more expensive than the financial losses. When one factors in the non-financial benefits of investing to prevent fraud, the cost-benefit analysis becomes even more clear.

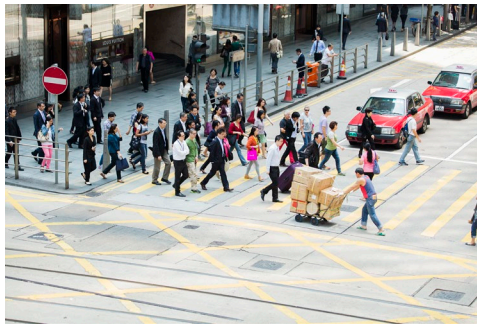
Investigating economic crime may be costly, but it's critical. It may result in asset or cost recovery. Tackling even the smallest crime can help a company learn lessons, uncover root causes, tighten up internal controls, and potentially avoid even bigger losses than if the fraud wasn't addressed. It is also a way in which to send a message to the organisation – if you commit fraud, we will take action.

Tomorrow's menu



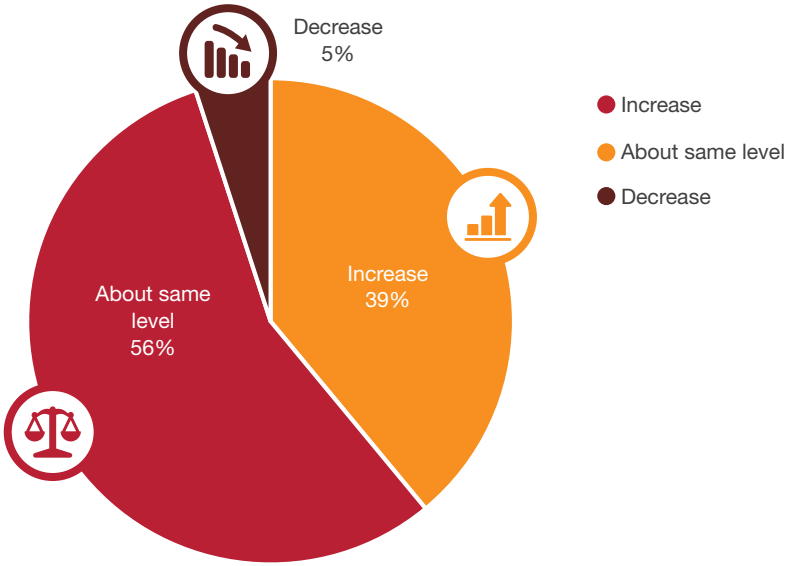
Southeast Asian respondents identified cybercrime (24%) as the crime they would most likely experience in the coming 24 months. This is in line with the global trend. Bribery and corruption (16%), asset misappropriation (11%) and business conduct/misconduct (11%) were all also identified as future concerns. We note, however, that only 21% of Southeast Asian respondents reported being the victim of cybercrime. With only 34% having undertaken a cyber vulnerability assessment in the last two years, it is quite possible that cyber-crimes have gone undetected.

Some countries such as Indonesia, Vietnam and the Philippines believe bribery and corruption to be the most damaging future threat, instead of cybercrime. This may be true, or it could be the result of a worrying lack of awareness of cybercrime, and organisations instead are still focusing on the threats of yesterday, rather than tomorrow's dishes.



Future expectations

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



Although many respondents believe they will suffer from some form of fraud and economic crime in the next two years, only 56% respondents plan to spend the same amount as in the last two years on their future anti-fraud efforts. Worryingly, 5% are actually planning on decreasing their budgets. Whilst these decisions are likely to be in part driven by financial necessity, there could also be a lack of appreciation for the severity of the threats they may face in the future.

Reluctance to embrace necessary changes may contribute to the significance of some of these threats. The trend of greater regulatory enforcement and inspection in Southeast Asia is expected to continue (51% of regional respondents believe regulatory activity will increase in the next two years). But there are still 19% of regional regulated respondents that have yet to carry out an Anti-Money Laundering or Combating Financing of Terrorism (AML/CFT) risk assessment. 18% of regulated respondents do not even know if their organisation conducts AML/CFT risk assessments.

Thankfully, there are positive signs in Southeast Asia too. Among the 19% of respondents that have yet to carry out AML/CFT risk assessments, 79% are planning to conduct one in the next two years. Additionally, regional governments have taken action in combating fraud. For example, Indonesia requires companies to publish their ultimate beneficial owners in an attempt to curb money laundering. Singapore has recently introduced the Deferred Prosecution Agreement for money laundering and corruption offenses.

Finding the discovery sweet spot

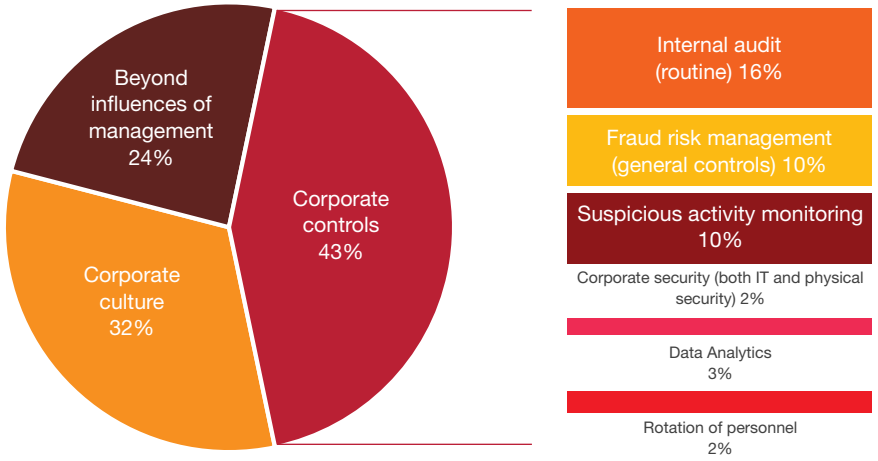
Historically, it was thought that the most that could be done about fraud was to react after the event. That does not mean that internal controls are a new concept, although it is true that approaches have historically been much more reactive than proactive. The manner of fraud discovery, whether it be proactive or reactive, often dictates how an organisation responds to fraud. Our study reveals that the majority of disruptive fraud incidents experienced by Southeast Asian-based organisations were initially detected by strong corporate controls (43%, proactive detection), followed by corporate culture (32%, reactive detection).

In Southeast Asia, corporate culture plays a significant role in fraud discovery. The 32% of fraud detected by corporate culture contrasts with 27% globally. This contrast is reversed when it comes to corporate controls, where 52% of global frauds (43% in Southeast Asia) were detected by controls such as internal audit and suspicious activity monitoring. This underemphasis on corporate controls in the region may indicate a potential blind spot for organisations in their fight against fraud and economic crime.

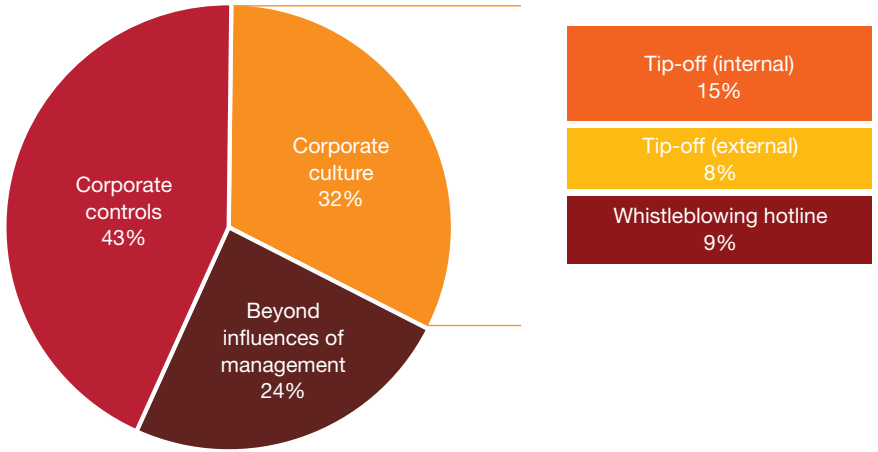
As with all things, a balance must be struck between proactive and reactive fraud detection. In any case, organisations will want to avoid instances of detection beyond their control - such as the intervention of law enforcement or the actions of investigative media. A significant 37% of frauds in Vietnam, for example, were detected by accident or through other activities beyond the influence of management. It can be very difficult for organisations to address fraud and deal with the potentially far reaching fallout if the first they hear of it is in the morning paper.

In today's digital age, corporate controls play a critical role in fraud discovery. As more and more transactions are documented digitally, assigning culpability for a potential misconduct may be difficult through traditional methods. Experience shows that disparate processes (e.g. internal controls), policies and procedures in organisations may increase the likelihood of misconduct, as well as the risk that it will go undetected. As crucial as reactive detection methods are in the fight against fraud, it is essential to remember the value that proactive detection can bring to any organisation aiming to be better prepared at facing fraud and emerging stronger from crisis.

How was the incident of the most disruptive fraud and/or economic crime that your organisation experienced initially detected? [Corporate Controls]



How was the incident of the most disruptive fraud and/or economic crime that your organisation experienced initially detected? [Corporate Culture]



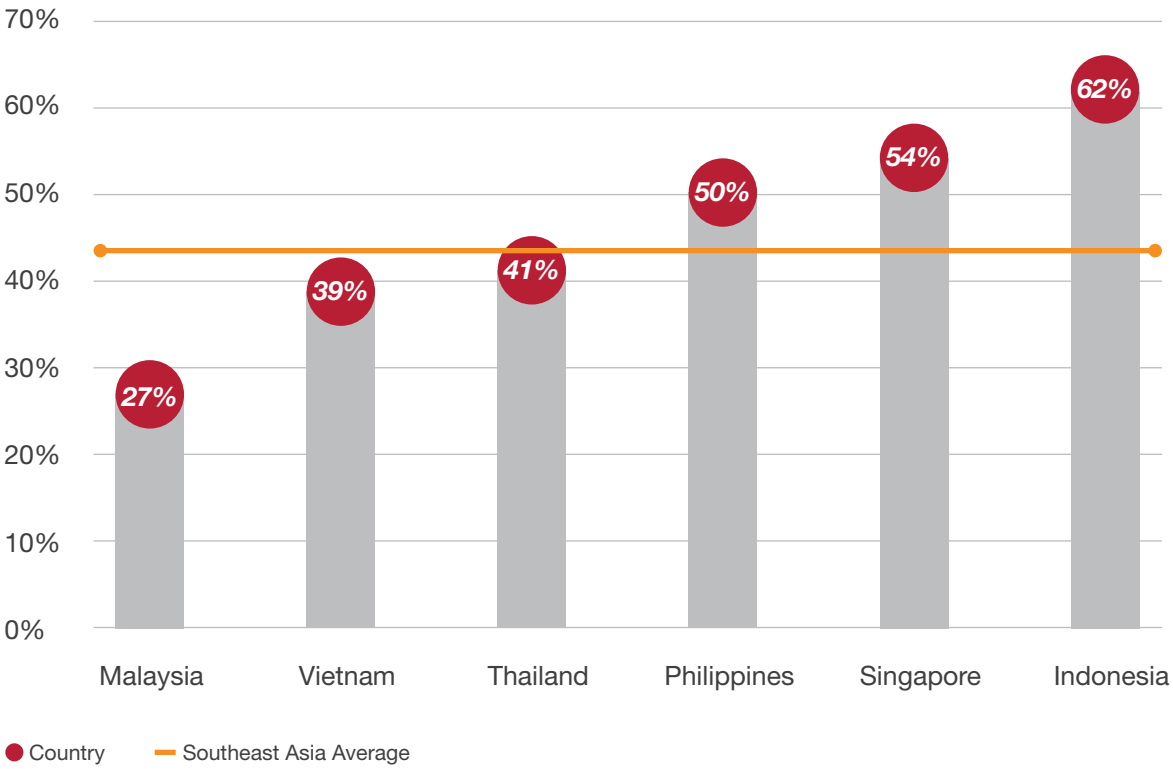
Hierarchy and its impact

Many local companies in Southeast Asia are either family owned or government run, and as such tend to have a hierarchical structure. 39% of our survey respondents represent these types of companies. As it's the tone and behaviour at the top of an organisation that sets the corporate culture, the right kind of hierarchy is vital.

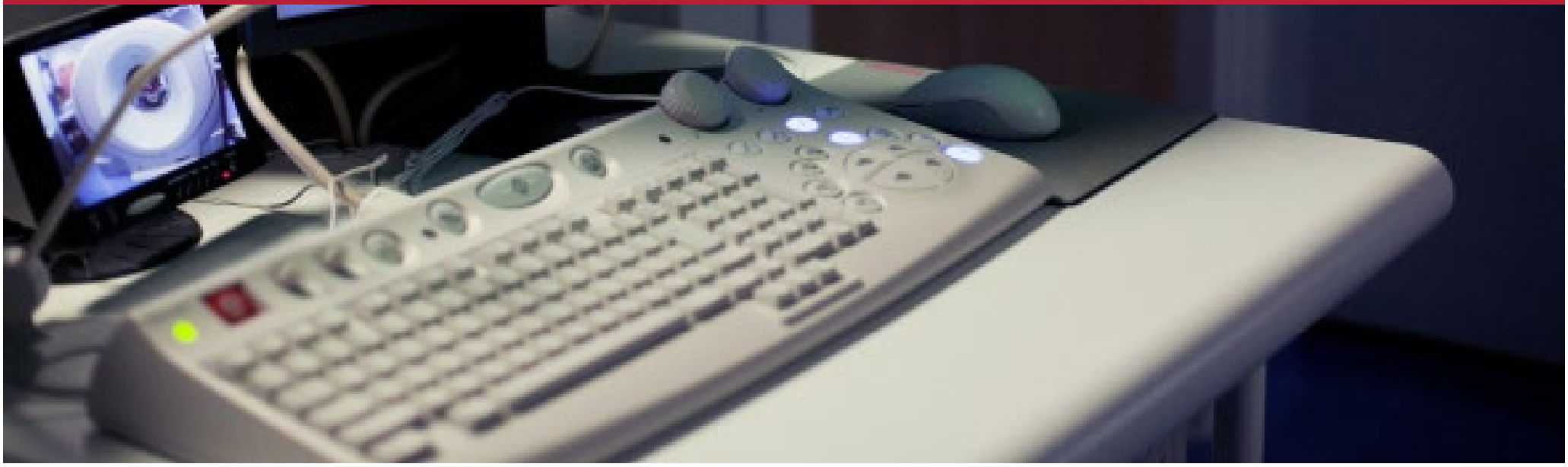
The right corporate culture help employees do the right thing by, for example, reporting suspicious behaviour. Whilst this is critical, it may not be enough to combat frauds. Among its regional peers, Malaysian respondents reported the lowest number of fraud initially detected through corporate controls (27%), significantly lower than the regional average (43%). A stark difference compared to some of its peers, Indonesia (62%) and Singapore (54%).

Strong hierarchies can often lead to a lack of empowerment at the lower levels of an organisation. In Southeast Asia, management styles tends to be more paternalistic. A strong hierarchical structure combined with the value of protecting one's culture may lead to a resistance to change - a potentially costly mistake in the ever-evolving fight against fraud.

Percentage of frauds detected through Corporate Controls in Southeast Asia, by country



Prevent and detect



Cybercrime - The invisible cloud looming over your organisation

As the crime predicted to be the most broadly suffered in the next two years both globally (26%) and regionally (24%), cybercrime is not a matter that organisations can turn a blind eye to. Global and regional respondents believe cybercrime to be the most disruptive crime they will face in the next two years. Globally, cybercrime was the second most reported crime over the past two years (31%), behind asset misappropriation (45%).

However, the results in Southeast Asia interestingly suggest that over the last two years asset misappropriation (52%), business conduct/misconduct (39%), bribery and corruption (29%), procurement fraud (27%), fraud committed by the consumer (25%), and accounting fraud (22%) were all more prevalent than cybercrime (21%). This seems to suggest that Southeast Asian organisations may not even be aware that they have been a victim of a cybercrime.

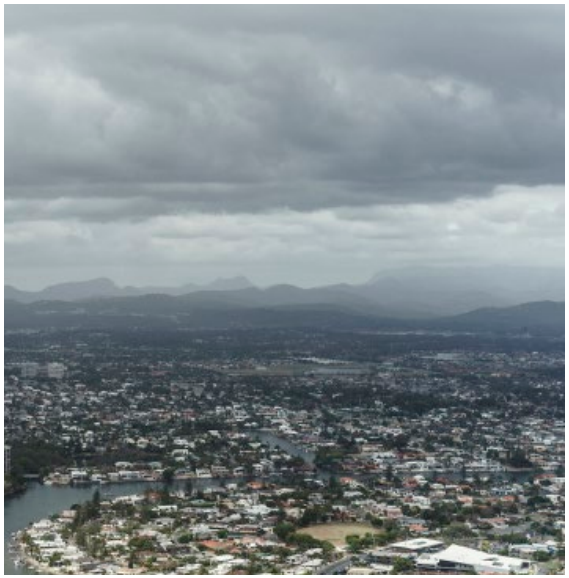
The results of the 2018 Black Hat Asia Survey[2] reveal a high level of uncertainty among enterprises about their ability to deal with current and emerging security threats. A majority of respondents to that survey doubt their organisation's ability to prevent major breaches from happening, and believe that a crippling attack on a major critical infrastructure target in the region is imminent.

What is cybercrime?

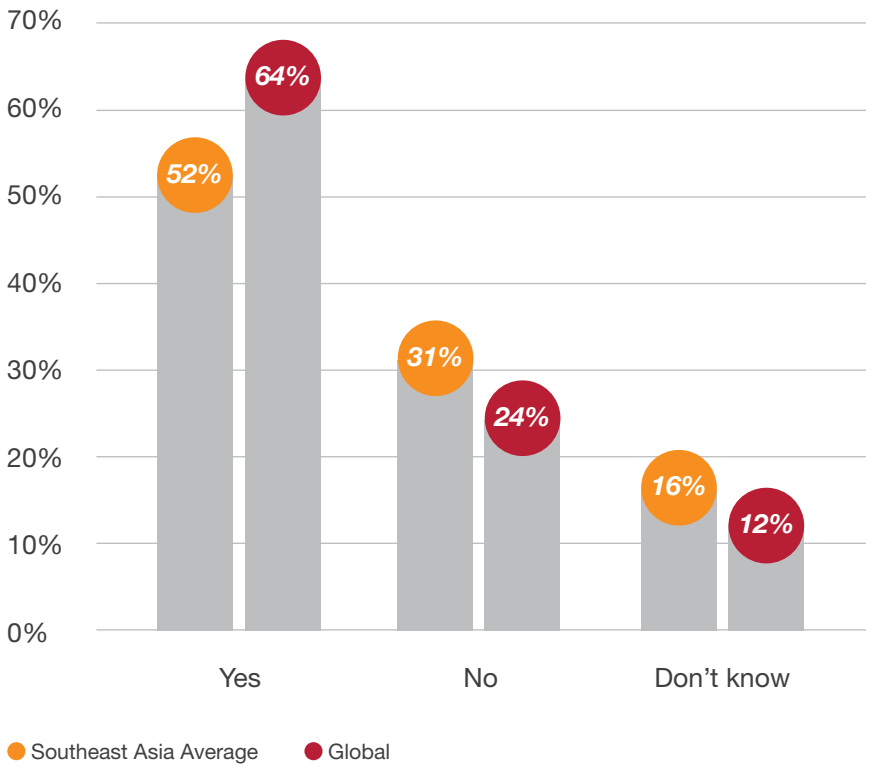
Any criminal offense committed by or facilitated through the use of computer equipment over a network.

What is a cyber-attack?

Malicious activity aimed at affecting the availability, confidentiality or integrity of computer systems for data.



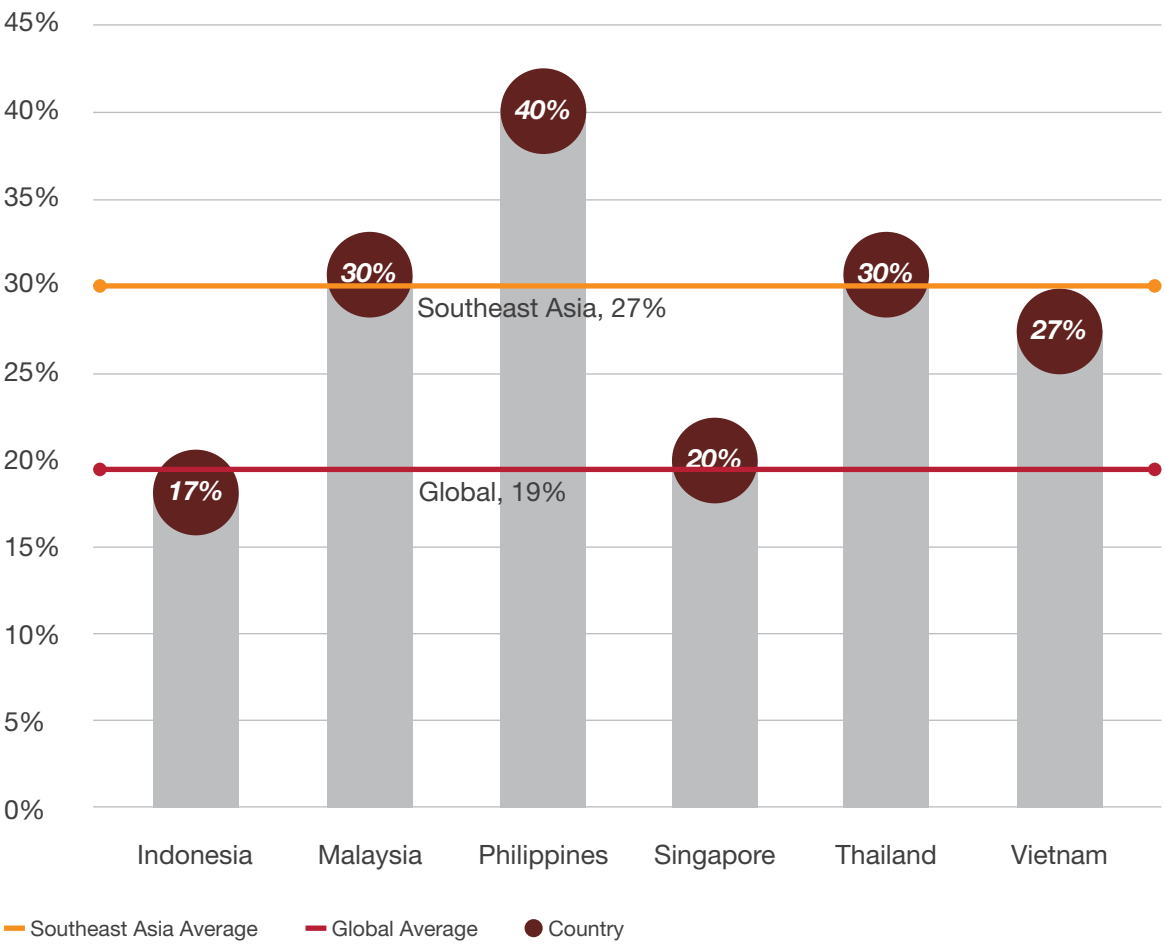
In the last two years, has your organisation been targeted by cyber-attacks?



[2]Black Hat is a well-known and established conference of cybersecurity researchers and enterprise information security professionals. Thycotic, a software company, ran the survey.

Cybercrime - The invisible cloud looming over your organisation

Percentage of Southeast Asian respondents that did not know the types of fraud and/or economic crime their organisations experienced through a cyber-attack



Phishing: Communications via email, SMS, telephone, etc., that, through the guise of legitimacy, seek information or place malicious software in an environment through a benign looking link or file.

Malware: Any form of malicious software that infects a network, servers, devices, or end user computers. Examples include ransomware, remote access tools, network sniffing software, and botnet software.

Despite the universally recognised threat, our survey indicates that only a small proportion of Southeast Asian respondents (34%) said that they had conducted a risk assessment on cyber-attack vulnerability. Disturbingly, 39% of Southeast Asian respondents either don't know whether they have a cyber security programme or confirmed they don't have a cyber security programme to deal with cyber-attacks.

It is apparent that organisations across the region are not well prepared to combat the anticipated cyber threat. Southeast Asian organisations should challenge themselves to stay on top of. Organisations need to be vigilant about cyberthreats and be aware of the measures their peers and competitors are taking to prevent, detect and respond to cyber attacks.

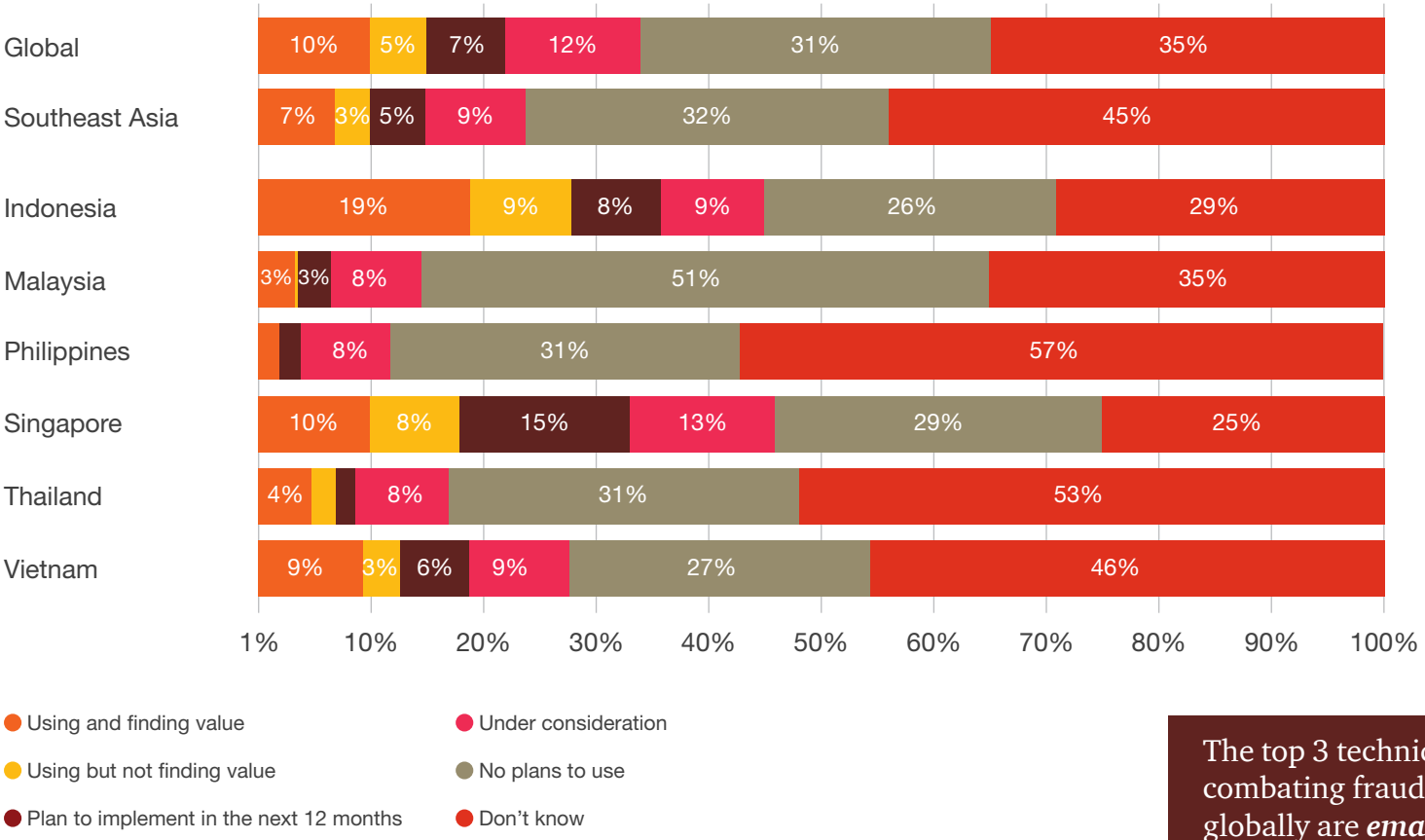
Global and Southeast Asian data show that the most common forms of cyber-attack are phishing and malware. In 2017, for example, there was a spate of highly disruptive cyber-attacks affecting companies across the region and around the globe, such as the so-called WannaCry and Petya ransomware attacks. Ransomware is a type of malware that prevents users from accessing their systems or personal files, and demands ransom payment in order to regain access. A majority of Southeast Asian respondents indicated that the cyber-attacks they suffered were related to disruption of business processes (29%) and extortion (26%), and a minority of respondents (5% globally and 4% regionally) think they were politically motivated or state-sponsored.

Cybercrime - The invisible cloud looming over your organisation

27% of Southeast Asian respondents revealed that whilst they were aware that their organisation had suffered fraud/economic crime, they were unaware what type of fraud or economic crime cyber-attacks had caused their organisation. Within the region, it is worth noting that 40% of respondents from the Philippines said the same, the highest in the region. These facts accentuate the complexity and obscure nature of cybercrime, as well as the technological dexterity required to understand, prevent and respond to cyber-attacks.

Artificial intelligence, advanced analytics, and you

To what degree is your organisation leveraging Artificial Intelligence or Advanced Analytics to combat / monitor fraud and other economic crimes?



Southeast Asia continues to grow as an economy, with the wider ASEAN region's GDP forecast to reach US$4 trillion by 2022.[4] However, the advent of "Industry 4.0," marked by the adoption of new technologies such as the Internet of Things, advanced robotics, 3D printing, and artificial intelligence (AI)/ augmented reality (AR) – based systems, could threaten this growth story in the longer term — unless regional markets start preparing themselves for the shift.

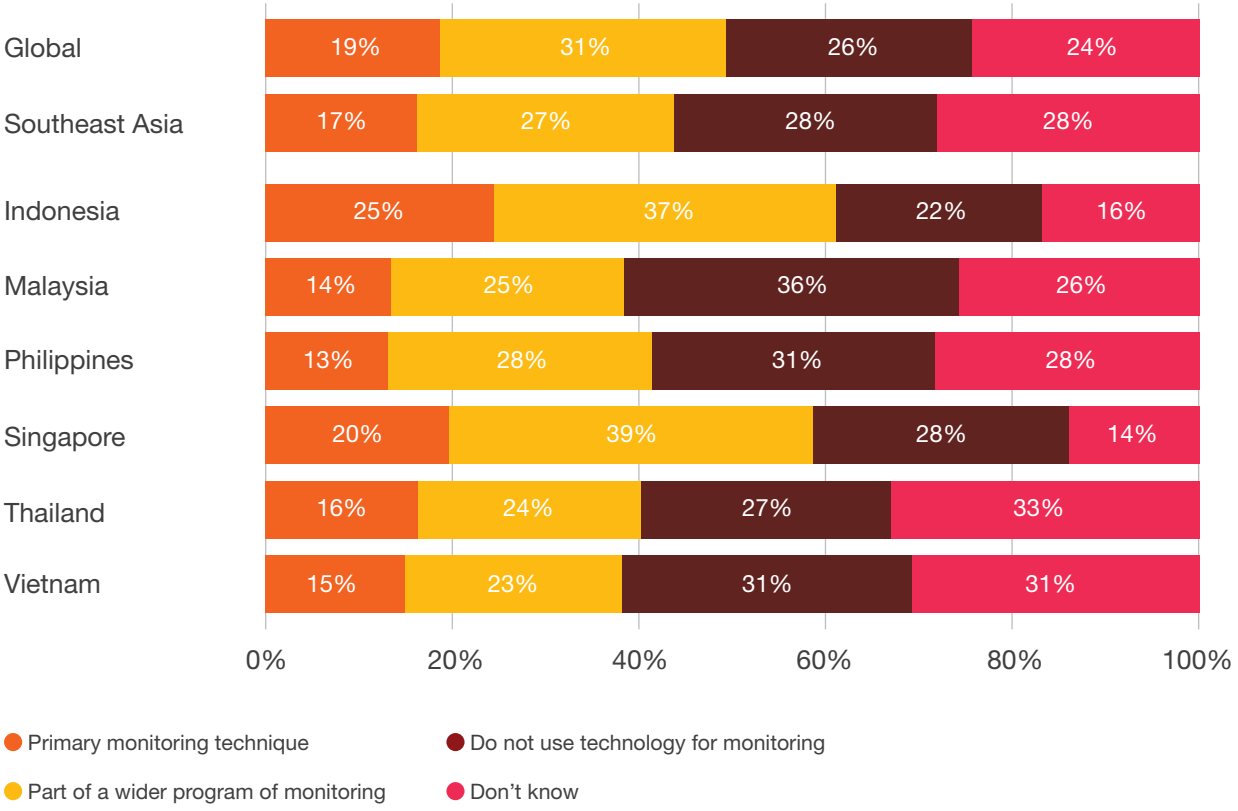
In an ever-changing digital world, where cyberthreats are constantly evolving, each more disruptive than the last, AI is a compelling game-changer, bringing the ability to detect and respond to threats as well as preemptively predict them. Whilst some Southeast Asian companies are leveraging AI or advanced analytics (7%), a disappointing 77% either don't know of any plans or have no plans to use AI or advanced analytics.

The top 3 techniques used and seen to be of value when combating fraud across the Southeast Asian region and globally are ***email monitoring, continuous monitoring*** and ***periodic analysis***

[4]PwC Growth Markets Centre, *"The Future of ASEAN – Time to Act"*, May 2018

Artificial intelligence, advanced analytics, and you

To what extent do you use technology as an instrument to monitor fraud and/or economic crime?



PwC's 21st CEO Survey[5] reported that 40% of CEOs across the world and 44% of Asia Pacific chief executives are extremely concerned about cyberthreats. Citing *PwC's 2018 Global State of Information Security® Survey*; 27% of executives say their organisation plans to invest this year in cybersecurity safeguards that use AI and machine learning. The more AI advances, the more its potential for cyber-attacks grows too. Techniques like advanced machine learning, deep learning, and deploying neural networks enable computers to find and interpret patterns. They can also find and exploit vulnerabilities. Cyber-attacks will be more powerful because of AI – but so will cyberdefense.

It's important for businesses across the region to understand that such investments in technology will not only serve to counter ever evolving cyber-attacks, but also help to fight fraud and economic crime more broadly.

Top three areas where technology was used as a monitoring technique to combat fraud within the Southeast Asian region:

- Cyber-attacks/Vulnerabilities (66%)
- Fraud detection (52%)
- Business Conduct (49%)

[5]PwC 21st CEO Survey, *"The Anxious Optimist in the Corner Office"*, January 2018

Technology

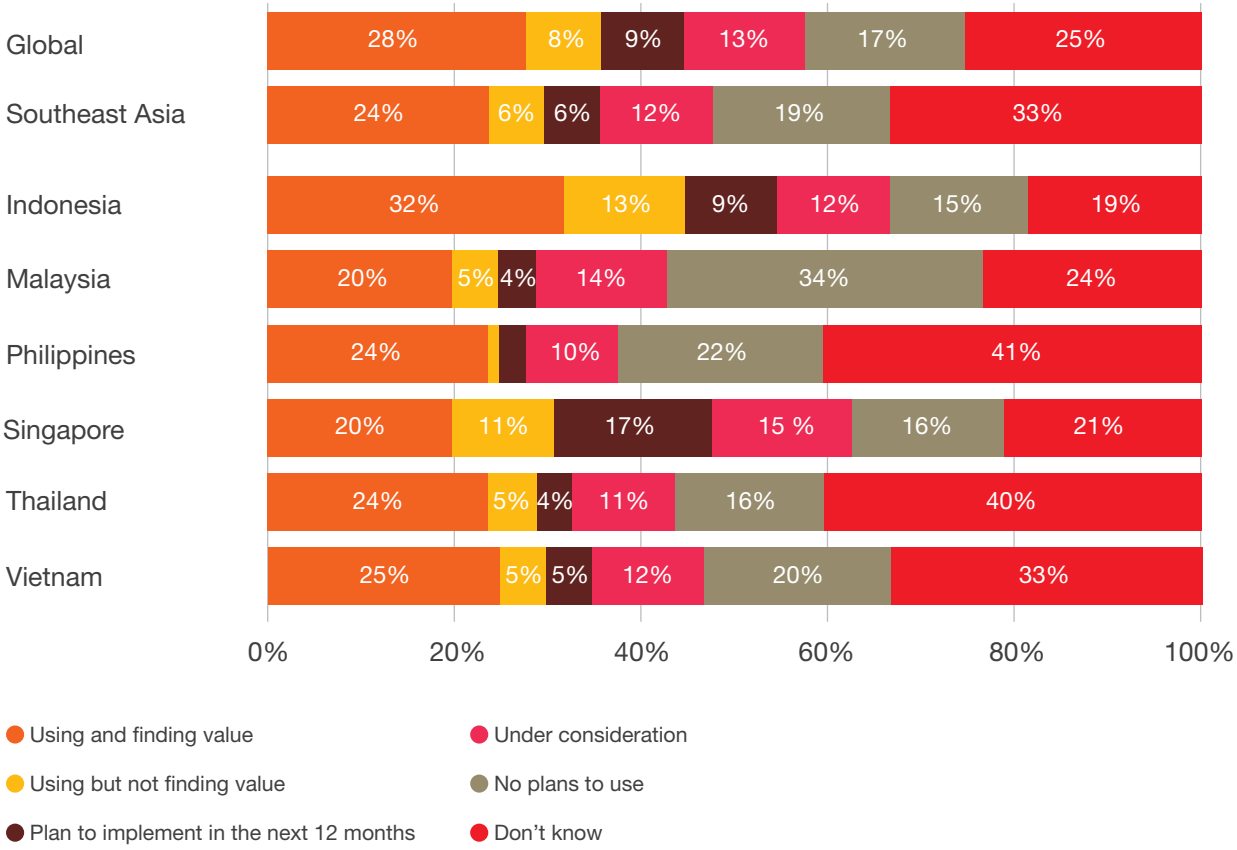
Embracing technology

Although Southeast Asia appears to be slightly behind the curve when it comes to embracing technology to fight fraud, some countries within the region appear to be leading the way. Indonesia (61%) and Singapore (58%) are already using technology to monitor fraud/ economic crime, either as a primary monitoring technique or as part of a wider programme, even higher than the global average (50%).

Many business processes could benefit from the deployment of anti-fraud technology, such as anti-money laundering (AML) and due diligence. 44% of Southeast Asian respondents are using technology-enabled techniques to combat fraud in different areas of their business. However, 75% of Vietnamese respondents do not know if they use, or do not use, technology to perform third-party due diligence on their business partners; the highest percentage in the region. In today's business world, it is not just a key component of a compliance programme, but a regulatory expectation to understand who you work with.

Embracing technology

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



Southeast Asian respondents say that they do see the value in using technology to combat fraud/economic crime. Making use of technology enables continuous real-time monitoring, provides actionable insight, integrates and manages necessary workflow or processes, to name a few advantages.

While many favour the use of technology in combating fraud and/or economic crime, 37% of respondents believes that it produces too many alerts or false positives. This can lead to customer friction - a growing challenge for organisations as they seek to strike the right balance between acting appropriately to fraud red flags and not being overzealous in alerting their customers, to the extent of causing irritation or impacting customer experience.

Public tolerance for fraud is diminishing

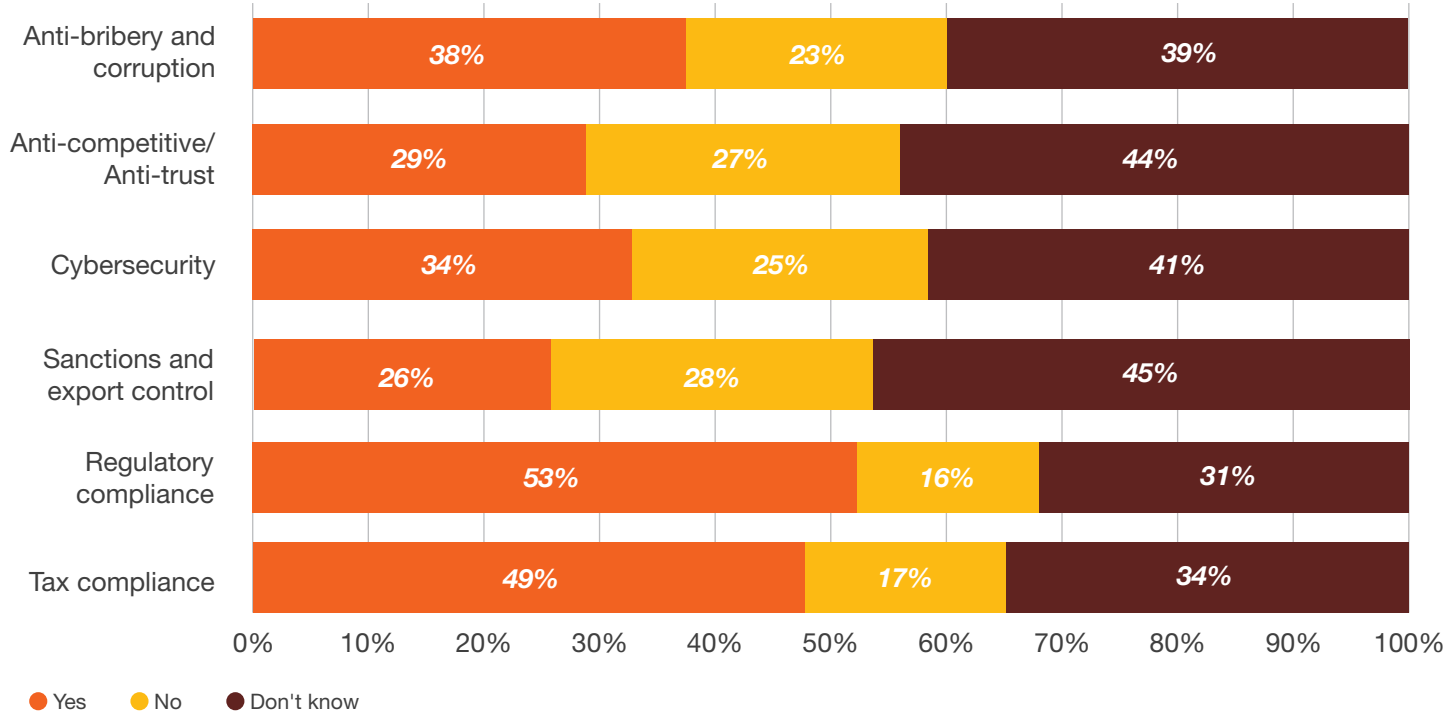
The public outrage caused by recent financial scandals in Southeast Asia indicates that public tolerance for corporate or personal misbehaviour is diminishing. This calls organisations to take a greater lead in preventing fraud before it can take root. Fraud risk assessments can help organisations to do so by identifying the specific frauds they need to look for. Besides increasingly being looked on favourably by regulators, these assessments also help companies be better equipped at facing fraud.

It is concerning that 12% of Southeast Asian respondents have not performed any fraud risk assessments at all in the past two years (compared with 10% globally). Whilst the majority of regional respondents have performed a general fraud risk assessment (57%, even more than the global average of 54%), more specialist assessment seem to have been forgotten. Encouragingly, however, 65% of Southeast Asian respondents confirmed they conduct regular risk assessments as a matter of course (comparing favourably to the global average of 60%).

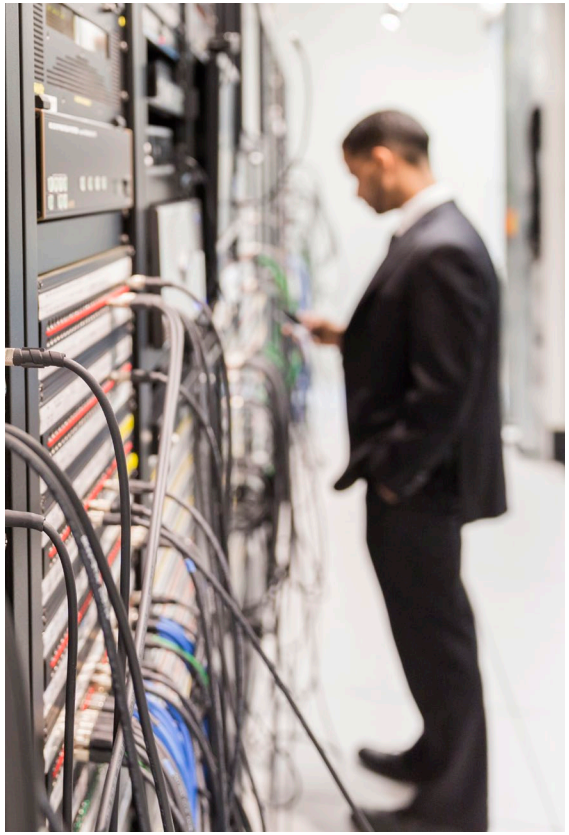
In the last two years, has your organisation performed a risk assessment on any of the following areas?

Public tolerance for fraud is diminishing

Does your organisation perform any of the following additional due diligence as part of your acquisition process?

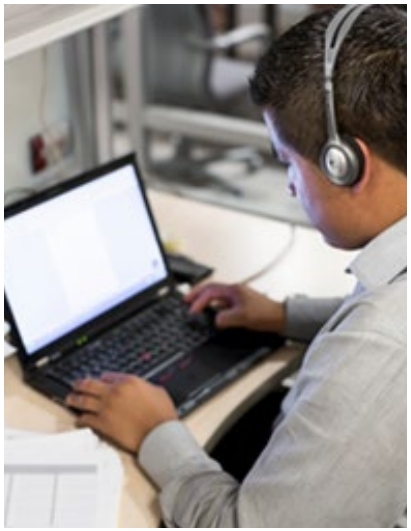


Another tool in the preventative arsenal is due diligence on third parties, such as vendors, targets for acquisition, or even potential future employees. Whilst regulatory or tax compliance due diligence is the most common (performed by 53% and 49% of regional respondents respectively), there are other forms companies should consider before engaging with a third party. Unfortunately, across the board Southeast Asian respondents take integrity due diligence less seriously than the rest of the world.



Unifying integrity

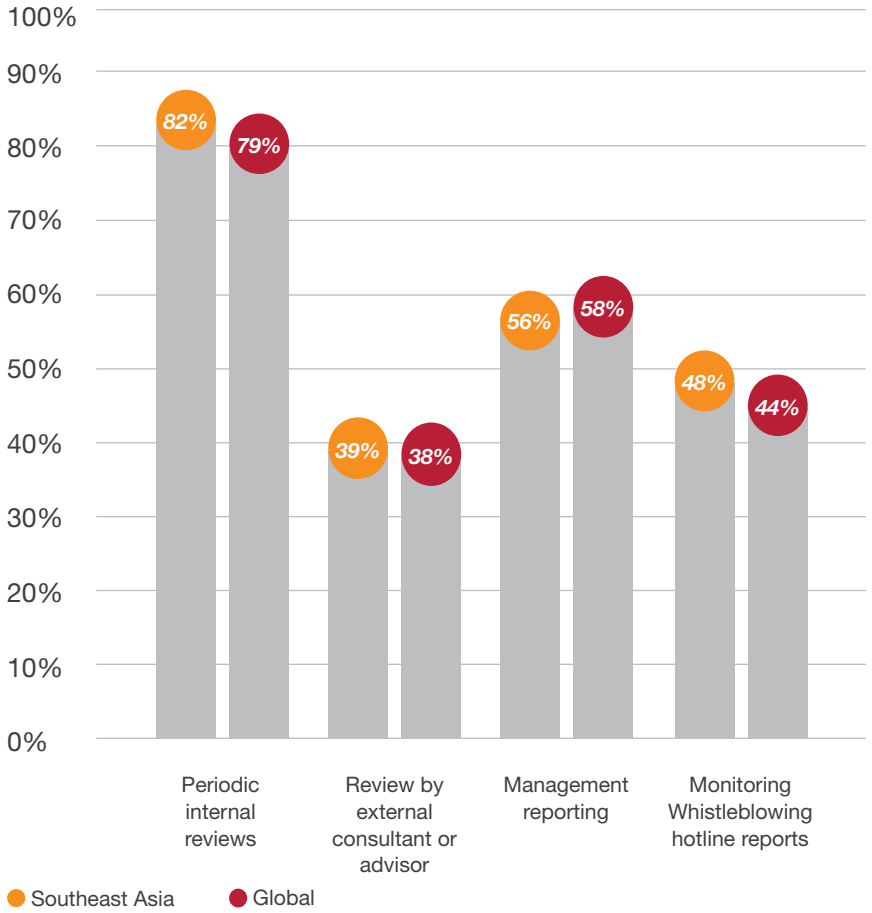
Corporate silos exist in most organisations. It is therefore no surprise that many companies treat compliance, ethics and enterprise risk management as separate functions, existing in separate departments with their own cultures and practices. Managing risks in a siloed manner can lead to duplicative efforts, with a lack of processes to take a holistic view. A better approach is one where risk management is a unified function of an organisation's strategy, with clear processes, practices and a culture. An integrated business ethics and compliance programme can help achieve this. 77% of organisations in Southeast Asia reported having a formal business ethics and compliance programme (in line with the global average). However, 10% of our regional survey respondents don't even know if their organisation has such a programme, double the global average of 5%.



Of those that confirmed they had a business ethics and compliance programme in place, 12% told us they had a dedicated team to tackle bribery and corruption, 31% had specific policies covering cyber behaviour, and 13% stated they had tailored controls in place for anti-money laundering. However, these data are consistently behind the global average (15%, 39% and 19% respectively), and 44% stated their programme either did not address competition/ trust risks or they didn't know whether or not it did.

A business ethics and compliance programme must be kept current and relevant. Southeast Asian respondents are better at this than the global average.

How does your organisation ensure that your compliance and business ethics program is effective?



Who takes responsibility?

Good practice encourages organisations to assign responsibility for the business ethics and compliance programme to a *Chief Compliance Officer (CCO)* or an equivalent role.

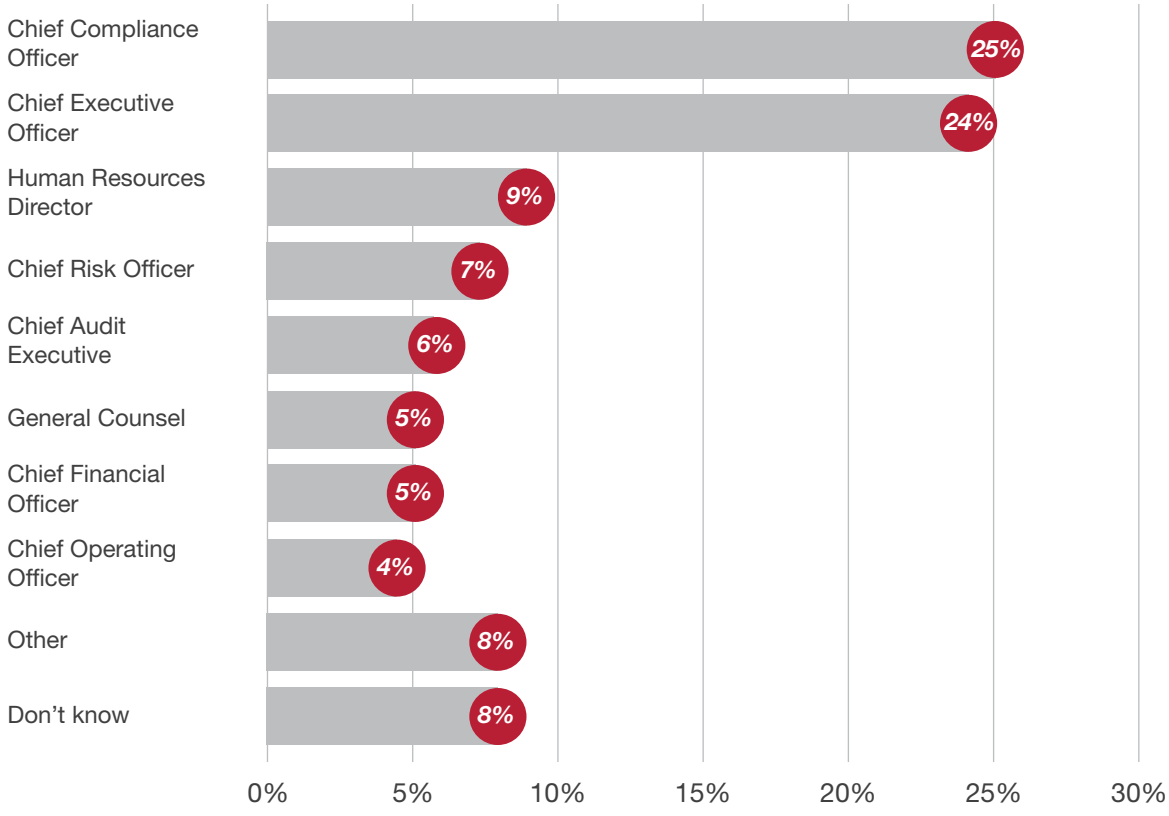
Where such a position does not exist, the role should be taken by a senior executive, such as the *CEO*.

In Southeast Asia, 25% of programmes fall under the CCO's remit (30% globally), and 24% under the CEO (17% globally). This regional difference is reflective both of the relative immaturity of business ethics and compliance programmes in the region, and the centralisation of power under the chief executive seen so often in Southeast Asian business culture.

When the financial costs of fraud hit the bottom line of a business, stakeholders naturally expect explanations from senior management. Unfortunately, a leader's responsibility does not stop there. A chief executive is often seen as the personal embodiment of an organisation. Increasingly, we see regulators willing to use their powers to take action against abuses of power by directors and CEOs.

One thing is clear: the C-suite are not invisible and can no longer claim ignorance as an excuse. Our survey shows that in Southeast Asia, in nine out of every ten cases, the most serious incidents of fraud have been brought to the attention of senior management. The fact that 24% of respondents indicated that the CEO has primary responsibility for their organisation's ethics and compliance programme puts a sharp spotlight on how the top office is managing crises. No longer is tone at the top sufficient. Stakeholders, regulators and the public as a whole are expecting the C-suite to demonstrate ethical behaviours at the top.

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

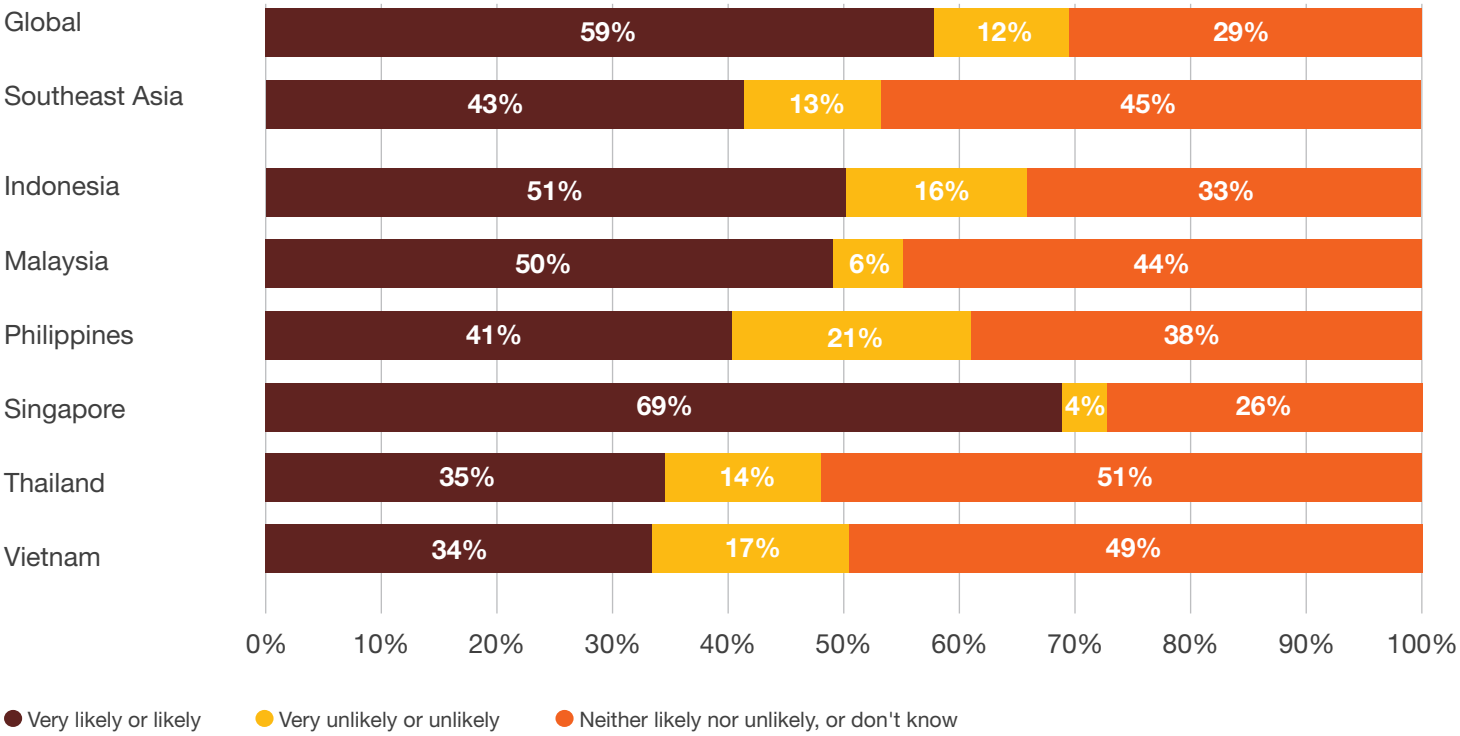


Technology - information sharing

A vital weapon in the anti-fraud arsenal is to keep abreast of the latest threats and vulnerabilities. This requires victims to share information about how they are being targeted, with law enforcement, private cybersecurity specialists, and each other.

Quite a promising 59% of global respondents indicate that their organisation would likely or very likely share information about suspicion of or actual cyber-attacks with government and law enforcement agencies. Regional respondents are not so optimistic. 45% of Southeast Asian respondents actually do not know whether they would share such information - or remain undecided. Our survey included a follow-up question into the reasons why an organisation might not share such information. 47% of regional respondents were concerned about the risk of uncontrolled public disclosure, perhaps indicating a lack of trust in their regulating authorities.

How likely is your organisation to share information with government/ law enforcement agencies about suspicion of or subjection to cyber-attacks?



According to Transparency International's Corruption Perception Index (CPI), the Asia Pacific region as a whole scores just 45 on the CPI. With a scale of 0 to 100, where 100 means very clean and 0 reflects a deep-rooted, systemic corruption problem, Southeast Asian countries are, on average, failing the corruption test. The Philippines has a 2017 CPI score of 34, its lowest score in the global corruption ranking in 5 years, slipping 10 places from 2016.

Prominently, 69% of Singaporean respondents were more inclined to share information with authorities, and this is in line with Singapore's 6th ranking on the 2017 CPI, making it the only Southeast Asian country in the top 50.

In a number of countries, it is the law to share information on cybercrime incidents with regulators. Sharing of information with the government and law enforcement agencies can contribute to a nation becoming more transparent.

Information is key - should details of cybercrime incidents be more widely shared, it could help organisations better prepare for future hacks. By sweeping cybercrime incidents and details under the carpet, we take away from organisations the benefits and opportunities to learn how to better protect their IT infrastructure in the future.

Emerge stronger

It is a sad but true fact of life that fraud and economic crime occurs even involving the most prepared of organisations. As this report has highlighted, these pains can be mitigated to some extent. Their impact can be limited by broad and early detection efforts through agile and technologically savvy organisations. Nobody can avoid them entirely however.

If the worst happens, there are many options open to organisations in their response. Examples might include: having a well designed and understood investigations process; employing suitably trained, independent and empowered investigators; providing full and rapid insight into the issues to business leaders; or effectively improving controls and processes found to have allowed the incident to occur in the first place. More important than just seeking to react to fraud, always on the back foot, is to proactively seize the opportunity to 'take the hit' and from it, to emerge stronger than before.

It is not enough for organisations to build their capability to withstand the financial and other damages of fraud and economic crime. Nor is blindly bulking up prevention and detection capabilities sufficient in today's globally competitive world. It can be tempting to simply sweep our problems under the rug, or go to great lengths to avoid confrontation. In the long run, these actions do nothing to strengthen an organisation, and in fact serve only to encourage bad behaviour.

When the worst happens, and we must all assume that at some point it will, organisations need to learn from it. Ensure that the right people and the right processes fully benefit from learning from the mistakes behind the incident, and that they and the wider organisation are truly empowered to develop and evolve in the best possible way in response. If organisations develop their ability to mitigate fraud risk based directly on fraud and economic crime already suffered, not only will they be better placed in the future, they will have reached that point more efficiently than their competitors.

There is an opportunity to turn the response to fraud and economic crime into a competitive advantage for the most prepared of firms. Aside from the obvious benefits of reducing fraud and economic crime such as limiting the direct and indirect financial pain, and limiting the non-financial damages of fraud, there are other, less tangible benefits. The kind of organisation that can 'bounce back' from fraud to emerge stronger has the culture and the infrastructure that allows it to respond to changes and challenges in the market more quickly than competitors. This culture has the added side benefit of going hand in hand with an ethical business mindset, helping to drive down the incidence of internally perpetrated fraud. These organisations have a higher 'breaking point' from fraud and other challenges than that of their competitors, allowing them to push further, take greater risks, and reap greater rewards.

The imperatives are clear. Ready your organisation for the next fraud. Prepare and empower your people, invest in technology and take the risk to respond - and **emerge stronger.**

Speak to us today

Richard Major
Partner, Southeast Asia Risk Consulting Leader
+65 6236 3058
richard.j.major@sg.pwc.com

Alex Tan
Partner, Malaysia
+60 (03) 2173 1233
alex.tan@pwc.com

Paul van der Aa
Advisor, Indonesia
+62 21 521 2901
paul.vanderaa@id.pwc.com

Chan Kheng Tek
Partner, Singapore
+65 6236 3628
kheng.tek.chan@sg.pwc.com

Vorapong Sutanont
Partner, Thailand
+66 (0) 2844 1000
vorapong.sutanont@th.pwc.com

Marcus Paciocco
Director, Vietnam
+84 24 3946 1609
marcus.paciocco@pwc.com

Roberto C. Bassig
Partner, Philippines
+63 (2) 845 2728
roberto.c.bassig@ph.pwc.com

Glossary of terms

Term	Definition
Audit completion/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).
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.
Bribery	The unlawful use of an official position to gain an advantage in contravention of duty. This can involve the promise of an economic benefit or other favour, the use of intimidation or blackmail. It can also refer to the acceptance of such inducements. Specific examples include kickbacks, extortion, gifts (with strings attached), facilitation payments, etc.
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.
Corruption	Dishonest or fraudulent conduct by those in power, typically involving bribery or conflict of interest.
Cybercrime	Any criminal offense committed by or facilitated through the use of computer equipment.
Cyber-attack	Malicious activity aimed at affecting the availability, confidentiality or integrity of computer systems for data.
Cyber Security programme	The people, processes and technology that assess, build, manage and responds to cyber security risk within an organisation.
Economic crime	The intentional use of deceit or other criminal conduct to deprive another of money, property or a legal right or to effectuate an economic harm.
Fraud committed by the consumer	Fraud against a company through illegitimate use of, or deceptive practices associated with, its products or services by customers or others (e.g. mortgage fraud, credit card fraud).
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 programme and controls in an organisation; and actions to remedy any gaps in the controls. Risk assessments can vary in scope, from broad, across the business assessments, to function, division or process specific. For example fraud risk assessments and cyber attack vulnerability assessments focus on fraud-specific risks and exposure to cyber attack, respectively.

www.pwc.com