Shining a light on fraud

Awareness is the first step towards fighting economic crime

pwc

www.pwc.com/crimesurvey


35%
37%
26%
2011
2014
2016

Contents

Foreword

Fraud and corruption have become increasingly well-publicised around the world in recent years. This has led to growing recognition from companies that these and other economic crimes can harm their ability to compete on the world stage, and has raised awareness at a country level that a transparent and clean business environment is essential for attracting foreign investors.

For that reason, I'm thrilled to be able to say that Thailand is leading the way when it comes to recognising the prevalence and danger of economic crime. In fact, more organisations from Thailand responded to PwC's *2018 Global Economic Crime and Fraud Survey* than from any other countries, showing just how seriously the issue is being treated here.

As this report shows, being aware of the risks – and talking about them – is the first step to defending against economic crime. Awareness also prepares companies to respond faster and more effectively if their defences are breached. This not only increases their chances of recouping losses through prompt legal action, it can also help them stop the incident spiralling out of control and potentially hitting their stock price, damaging their reputation with consumers and/or business partners, or attracting penalties or other censure from regulators.

pwc

I believe this willingness to talk about economic crime in Thailand is driven in large part by changes to this country's business culture as we increasingly embrace globalisation, openness and transparency.

I'm proud to say that PwC has been an active partner in this change. In 2009, we established PwC Forensics as the first professional services team in the country to have a primary focus on preventing, detecting and investigating economic crime. Since then, the team has been raising awareness of economic crime and what to do about it through presenting at business conferences and talking directly with organisations and professional bodies to help them put in place defences against economic crime.

This expertise is based on knowledge chipped from the coal-face during countless investigations into financial statement fraud, asset misappropriation, commercial bribery, kickbacks and cybercrime, as well as through helping companies comply with anti-corruption and anti-money laundering legislation.

I welcome you to read this report and join the conversation about economic crime and fraud. With awareness, together we can fight the scourge.

Sira Intarakumthornchai
Chief Executive Officer, PwC Thailand

Preface

Our *2018 Thailand Economic Crime and Fraud Survey* is as much about the crimes you don't see as it is about those you know have affected your business.

The percentage of survey respondents in Thailand who said that they'd been the victim of economic crime and fraud in this 2018 report was almost doubled the corresponding rate in the 2016 report, increasing from 26% to 48%.

At first glance, this indicates that fraudsters are winning the battle and that economic crime is on the rise. However, on deeper inspection, it's clear that what we're in fact seeing is that economic crime is being dragged out of the shadows and into the light.

The increase indicates growing *awareness* of economic crime and fraud rather than growing *incidence* and *victimisation*.

This is a good thing.

Those of us on the front line of fraud prevention, detection and investigation are accustomed to fighting against an invisible enemy. We know that acknowledging that the fraudsters are out there, even if we can't see them, is the first step towards winning the war. And this survey shows that organisations are taking this first, all-important step.

pwc

Organisations that recognise fraud, corruption and other economic crimes as a part of a shadow industry with tentacles in every country, sector and business function are in a strong position to invest in the people, business processes and other tools they need to effectively minimise their exposure. Those that do not acknowledge the hidden risks that this shadow industry poses to their organisation are in a dangerous position.

So the important question isn't: *Are you a victim of fraud?* The important questions are: *Are you aware of how fraud is affecting your organisation?* and *Are you fighting it blindfolded, or with your eyes open?*

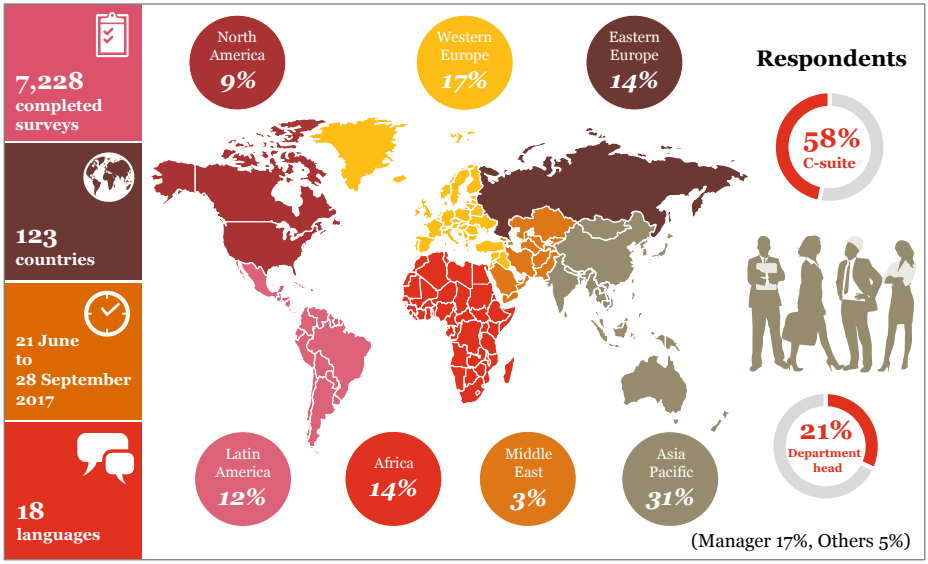
The economic crime you don't see is as important as the crimes you do see. This is the focus of our report. We explore not only what is visible, but also the blind spots that are hindering companies from seeing the fraud in their midst, and what they can and should do about these blind spots.

Vorapong Sutanont
Partner
Forensic Services, PwC Thailand

Section 1

Awareness of economic crime is growing, but how much still remains in the shadows?

Size, scale, and depth of the global 2018 survey

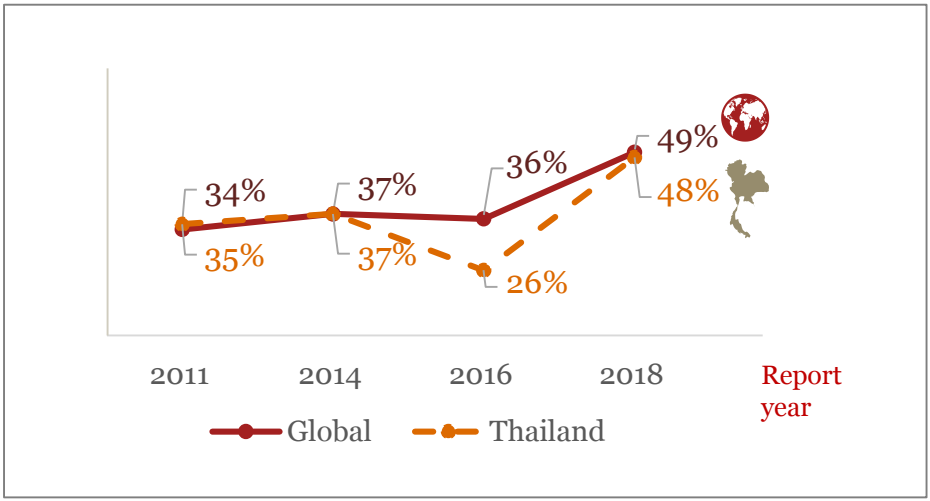


Thailand's response to PwC's *Global Economic Crime and Fraud Survey 2018* threw up an extraordinary finding – 48% of the respondents said that they'd experienced economic crime in the last two years, almost doubled the percentage in 2016. A smaller but still significant jump was also seen globally, with experience of economic crime climbing from 36% to 49%.

Has economic crime in Thailand – and around the world – really increased that much, or is something else going on below the surface? Something we can't quite see?

Our experience at the front line of the battle against economic crime and fraud tells us that it's most likely the latter. We suspect that the difference between the two surveys is not due to any significant change in the *incidence* of economic crime and fraud, but that it represents a growing *awareness* of fraud.

Reported rate of economic crime – globally vs. Thailand



We believe – and our work largely confirms this – that practically every company has suffered losses from economic crime at some time and to some extent. But in too many cases, it goes undetected or unreported. All businesses are vulnerable. Often the losses are minor – which is a key reason why they go undetected. But low-level crime can lead to bigger loss and more lasting damage as the perpetrators get bolder in their schemes, potentially recruiting others to help orchestrate a bigger conspiracy.

The increase in awareness is an encouraging sign, and one that can make a real difference in the fight against fraud, both for individual companies and for Thailand as a whole. However, we'll really know that we are making inroads when the reporting rate to our survey is closer to 100% when detection of fraud is much more prevalent.

Based on our experience, we believe that Thai companies are increasingly willing to talk about economic crime. This willingness is driven in part by changes to the country's business culture as Thailand increasingly embraces globalisation, openness, and transparency.

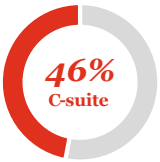
The willingness to discuss the issue is demonstrated by the incredible survey response we had in Thailand. More companies responded than in any other country, giving us great insight into the extent of economic crime and fraud here, its impact, and what companies are doing to prepare and respond to it. Of more than 7,200 completed surveys across 123 countries, 522 were from Thailand. This rate is well ahead of the next highest country, the United States with nearly 350 completed surveys.

Almost half (46%) of the responses in Thailand were from the C-suite, and 22% were from department heads, including those with finance, audit, compliance, and risk management functions. This indicates that concern about economic crime is being prioritised at these companies.

The industrial sector accounted for almost half (46%) of the respondents, in part indicating the importance of manufacturing and exports to the Thai economy. But it also shows that these companies are waking up to the extent to which their long supply chains and multiple contact points with third party vendors – which are often handled by mid-level managers and lower – leave them vulnerable to economic crime and fraud.

Size, scale, and depth of the Thailand 2018 survey

Respondents



71% manage Finance, Executive Management, Audit, Compliance and Risk Management, and Fraud and Financial Crime functions

42% work for multinational companies

55% work for companies with more than 1,000 employees, 32% of which work for companies with more than 5,000 employees

51% work for publicly traded companies

33% work for privately owned companies

(Manager 25%, Others 7%)

Industries

21% Manufacturing

19% Financial services

6% Insurance

6% Retail and consumer

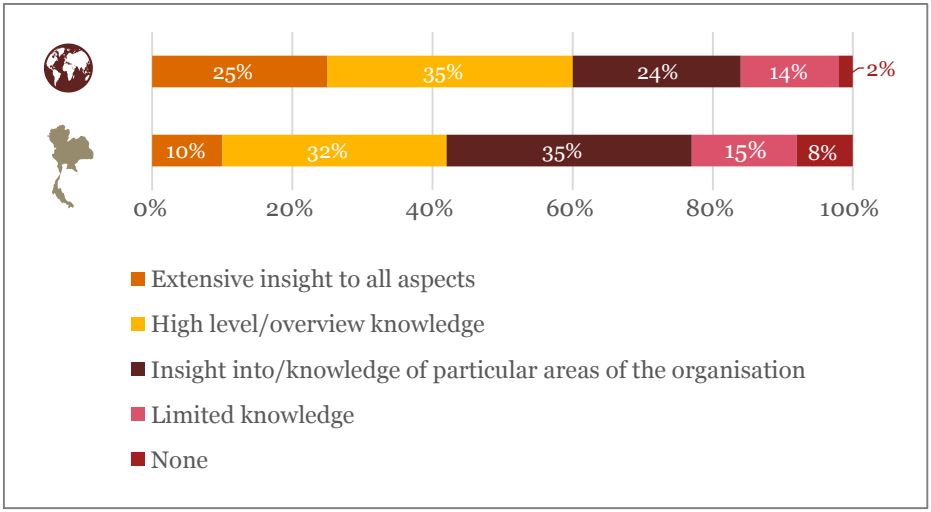
6% Technology

Financial services and insurance companies were responsible for a quarter of responses. While this percentage is down from the 2016 survey, it's simply due to a much higher response rate from the industrial sector. In fact, the number of financial sector respondents increased. This shows that financial services companies are as aware as ever of just how prime a target they are for fraudsters.

But here's the question: *Aside from talking about the need to address economic crime, are companies actually making the shift from a traditional reactive stance to a more proactive one?* Or *are we still missing something vital in the fight against fraud?*

Our survey results strongly suggest the latter.

Knowledge of economic crime – globally vs. Thailand



Awareness is growing, but the complete picture is missing

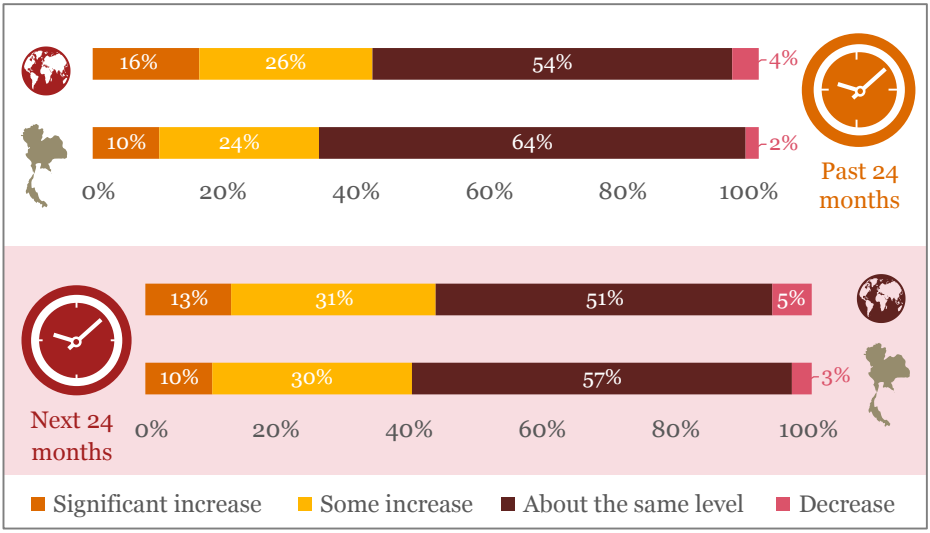
Our survey shows that even while awareness is rising, too many companies here still have only limited insight into their economic crime. Alarmingly, only a small proportion of respondents in Thailand confidently said that they have extensive insight into all spectrums of economic crime within the organisation. Overall, we are still trailing behind the global average in being forefront and recognising what is happening within our business operations.

Given the risk of limited visibility, we want to see these numbers change significantly over the next two years.

Notably, 35% of respondents in Thailand said that they have insight only into particular areas of their organisations, compared to 24% globally. This could indicate that people are working in silos when it comes to compliance, ethics, and risk management.

Because fraud is so easily brushed under the carpet or seen as 'someone else's problem', uncentralised fraud prevention effort exposes companies to greater risk. Winning this fight requires a broad, holistic, enterprise-wide approach.

Funding of fraud and economic crime prevention – globally vs. Thailand



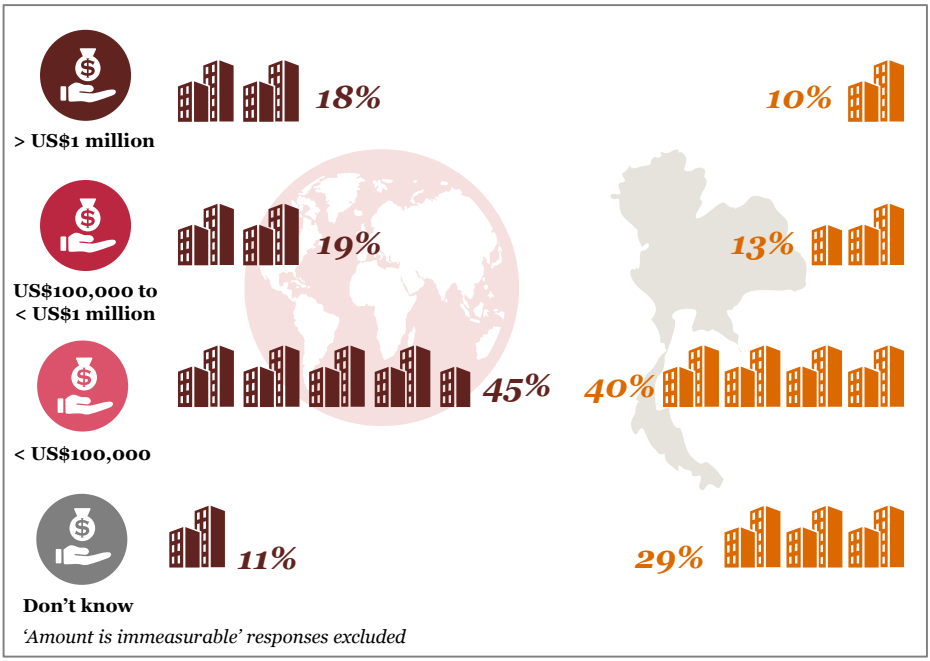
Costs can be crippling, so why is investment in prevention lagging?

Given the potential costs, too few companies are committing additional funds to combat economic crime. The majority of Thailand respondents (64%) hadn't increased the allocation of corporate budgets used to combat fraud and economic crime in the last two years, and 57% don't intend to over the next two years.

Only 10% increased funding significantly over the last two years, and only 10% plan to do so over the next two years.

Almost a third of the Thailand respondents (30%) plan some increase over the next two years, which is up from the 24% in 2016. This compares marginally unfavourably with 44% of respondents globally who plan either a significant increase (13%) or some form of increase (31%) over the next two years.

Direct loss to most serious economic crime incident – globally vs. Thailand

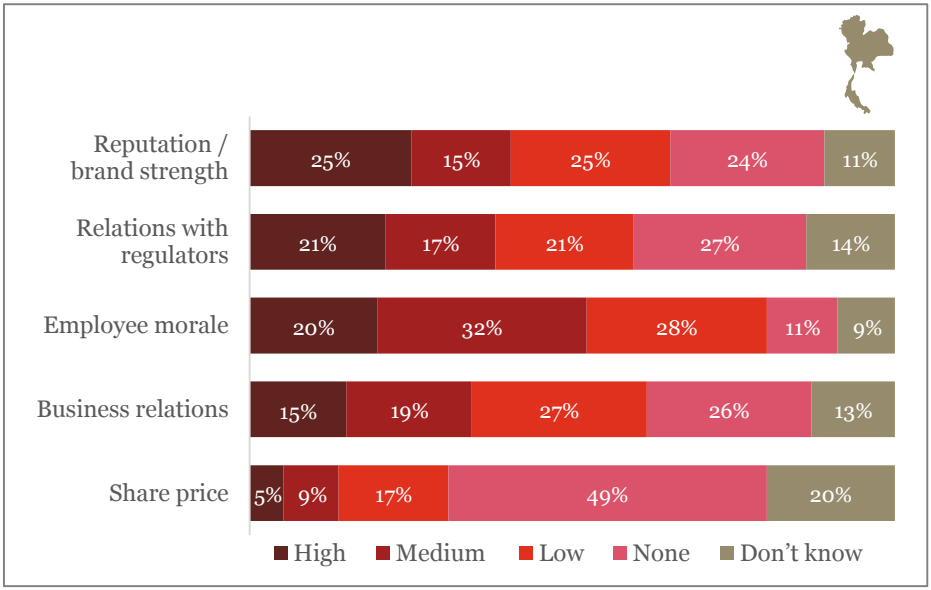


We believe that there's a significant return on investment in fighting economic crime given how extensive and severe the losses can be. Ten percent of Thailand respondents said that they lost at least US$1 million from the most disruptive crime which they suffered in the last two years. One respondent estimated the loss at more than US$100 million. Four lost between US$50 million and US$100 million, and 21 lost between US$1 million and US$50 million.

Thirteen percent lost between US$100,000 and US$1 million, and 40% lost less than US$100,000.

Almost three in ten respondents (29%) weren't able to estimate how much their companies had actually lost.

Impact of economic crime on companies in Thailand



Your business depends on how people see you

But the cost isn't just financial; indirect losses can also be significant. From their experience with the most disruptive economic crime, 25% of Thailand respondents said that their reputation and brand strength was most impacted. Another 15% said that the impact was medium.

Globally, survey respondents consistently ranked reputational harm at or near the top of the negative effects of economic crime, with public perception (which includes reputation, brand strength, business relations, and share prices) taking the hardest hit. This impact has continued to increase since 2016.

Reputation can take years to build, but it can be shattered almost instantly if companies fail to prepare or respond adequately to address an issue. Because bad news travels fast, this can happen before the management board even has a chance to assess the possible damage and plan on what to do.

To ensure a quick response, companies need to develop a crisis management plan, and define when it's necessary to put it into action. A virtual team needs to be created to manage the response, and all stakeholders should be made aware of what to expect if a crisis does hit.

You need to prove you're doing things right

Thailand respondents said that the crime impacted their relations with regulators, with 21% rating it as highly disruptive to these relationships, and 17% rating it as a medium impact. To compete under increasing regulatory scrutiny, you want to make sure that the regulators know you're proactively in control.

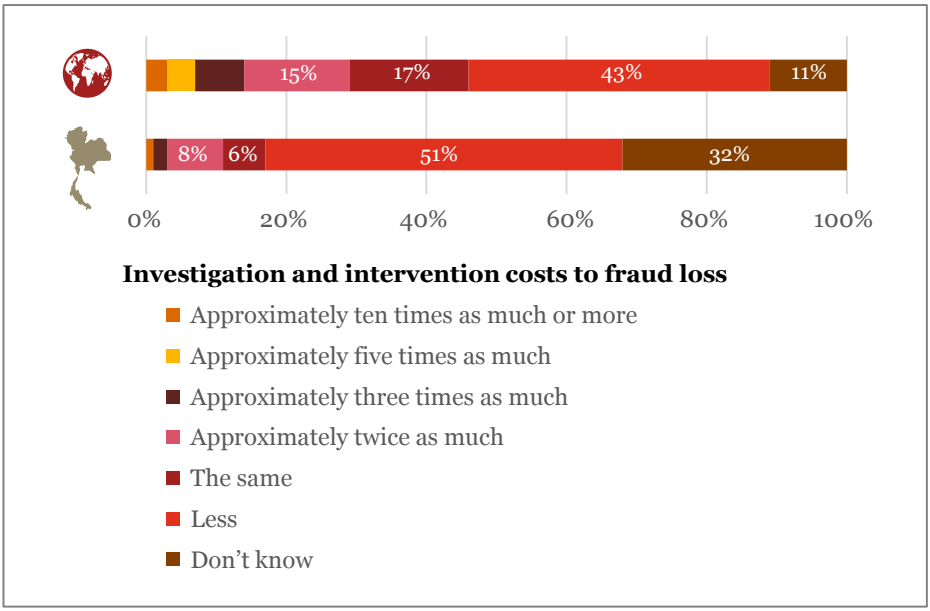
The people working for you need to trust you

Economic crime impacts employee morale. Of the Thailand respondents, 20% said that the crime had a high impact on how employees felt about their company and 32% said that it had a medium impact.

Employees who act in good faith feel let down by a corporate culture or internal controls that allow fraud to occur. They may be placed in a stressful position of deciding whether to blow the whistle or to stay silent.

Likewise, if the perpetrators continue to get away with the crime, there's a big risk that other ethically mediocre staff may decide that it's not a big deal and no one cares anyway, and commit fraud themselves.

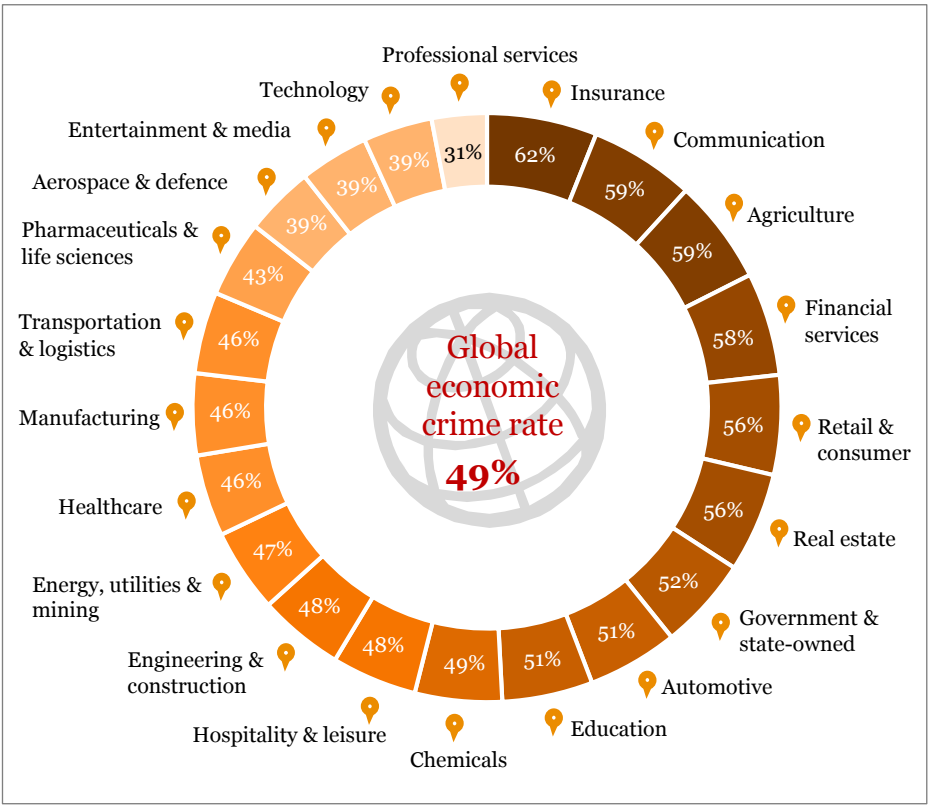
Investigation and intervention costs for the most serious economic crime incident – globally vs. Thailand



Investigating economic crime may be costly, but it's critical. It can even 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 avoid even bigger loss from the perpetrators who are continuing with the fraud schemes.

While 51% of Thailand respondents spent less on investigating the crime than what they lost to fraud, three respondents spent ten times or more, and 10% spent two or three times as much. A large percentage (32%) said that they didn't actually know how much they'd spent it, compared to just 11% globally.

Global percentages of economic crime incidents by sector



Section 2

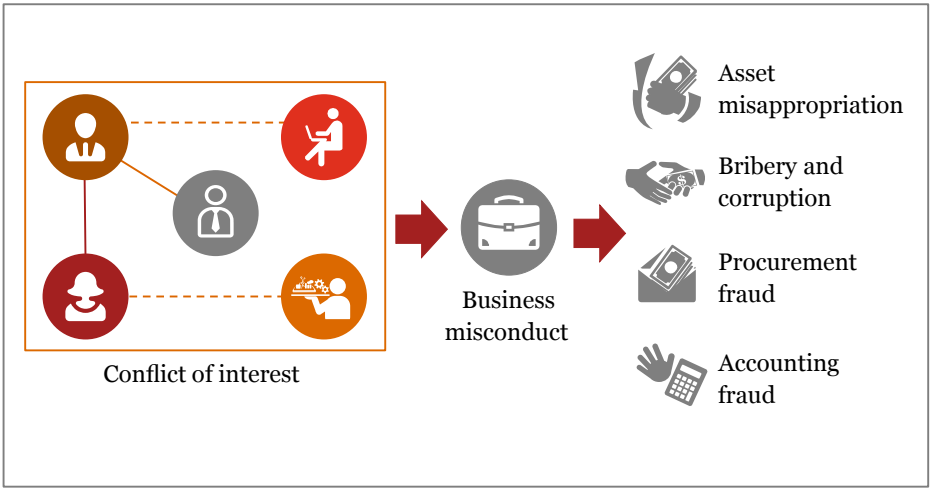
Know your fraud, and don't forget to look at those who do business with you

Fraud can manifest in many different ways and can affect many different parts of an organisation. A one-size-fits-all prevention strategy may leave blind spots for fraudsters to slip through.

In the 2018 survey, some types of fraud were included as separate categories for the first time in response to their growing prominence. Of these, business misconduct was the second most common fraud which Thai companies experienced in the last two years, with 40% being affected. Just 16% said that it was the most disruptive crime they'd experienced.

Business misconduct

Business misconduct refers to a wide range of improper behaviour, from false timesheet entries to bid-rigging to favouring a friendly party. It's the suspicious behaviour that tests the strength of the company's commitment to fight fraud. Often, it's the first symptom of more serious problems, such as corruption, asset misappropriation, accounting misrepresentation, and procurement fraud.



Thailand's business misconduct score is much higher than the global number (28%). This suggests that internal fraud prevention policies might have gaps, grey areas, or loopholes that can be exploited with little fear of legal action.

In our experience, we've found that Thai companies are particularly vulnerable and exposed to conflict of interest schemes, a classic type of business misconduct.

Fraud by consumers involves illegitimate use of, or deceptive practices associated with, a company's products or services, such as mortgage or credit card fraud.

Fraud committed by consumers

This new category in the survey affected 23% of Thai companies compared to 29% globally.

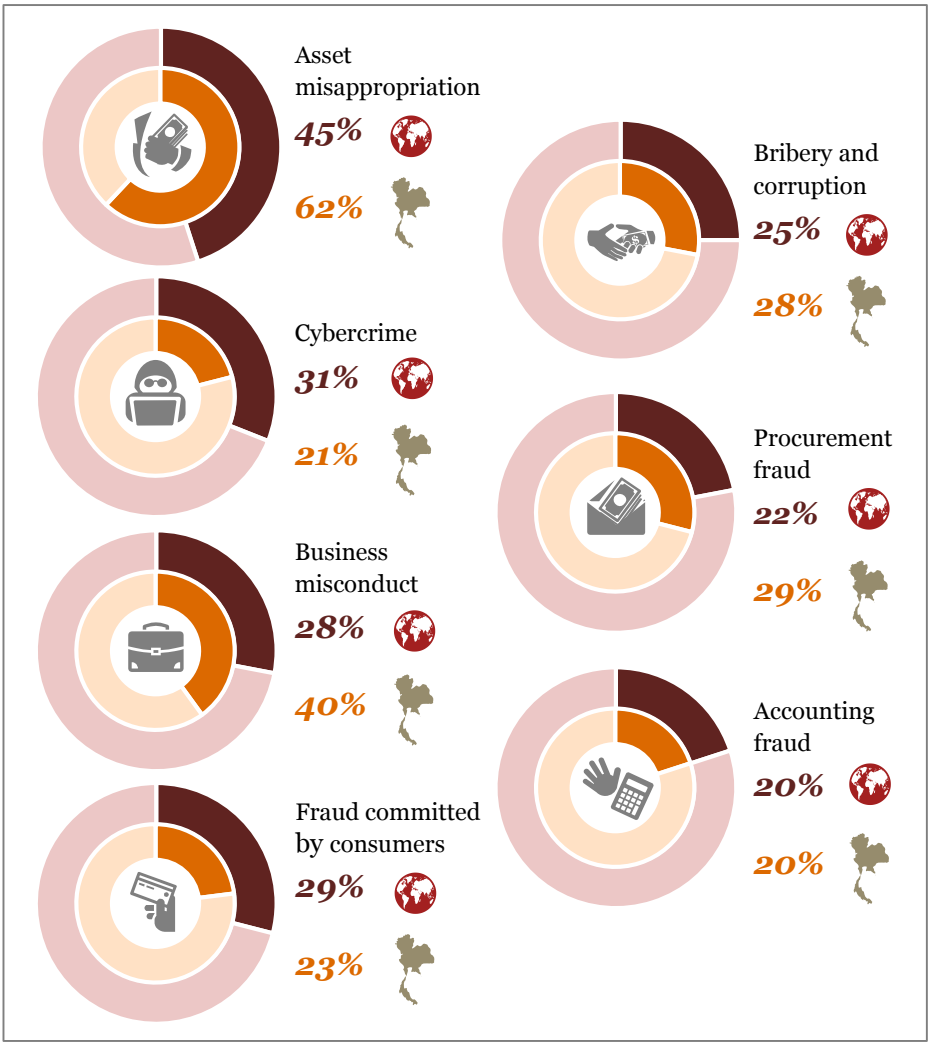
Asset misappropriation

Asset misappropriation was again the most common economic crime in Thailand, affecting 62% of respondents. A little more than a quarter (27%) said that it was the most serious crime that they'd experienced. This is down considerably from 78% in our 2016 report, but it still remains a significantly bigger issue in Thailand than it does globally (64% in 2016 down to 45% in 2018). We think that this is in part due to the large portion of respondents coming from the industrial sector, where asset theft is more prevalent and the assets are of commercial value.

Procurement fraud

Procurement fraud is also in the top five categories in Thailand at 29% compared to 22% globally. This is an increase on the 18% in 2016. From our experience, industrial sector companies are particularly vulnerable to this type of fraud.

Most common types of fraud and economic crime experienced by companies – globally vs. Thailand



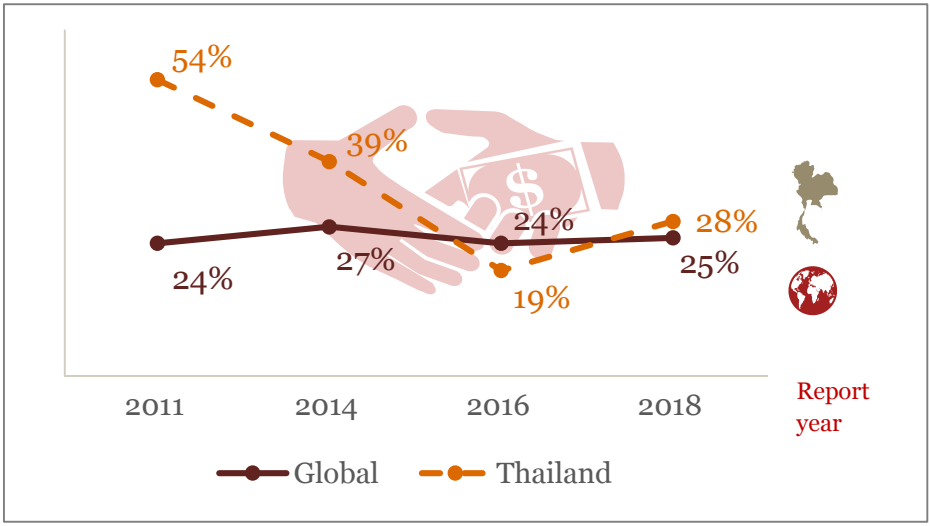
Bribery and corruption

Bribery and corruption is a serious issue in Thailand with more than a quarter of respondents (28%) saying that they've been affected by it in the last two years. Our experience suggests that it's significantly under-reported.

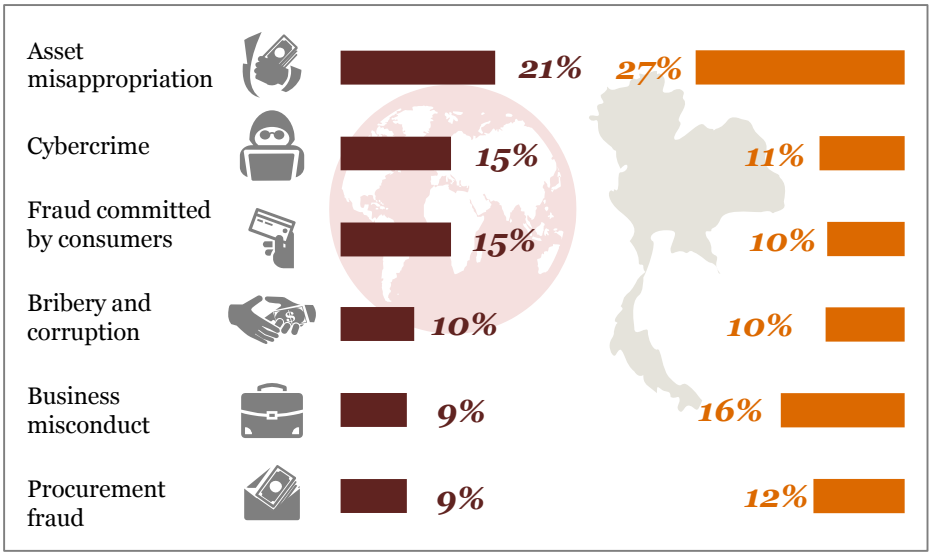
This seems to be recognised at the national level as Thailand is putting serious effort into combating it. The *Thailand Private Sector Collective Action Coalition Against Corruption* was launched in 2010 to boost awareness of corruption risk and put in place anti-bribery and corruption policies and mechanisms to prevent corruption in the private sector.

Although the percentage rose slightly from the 2016 report, we hope to see the impact of the coalition and other measures start to show over the coming years.

Percentage of companies who experienced bribery and corruption – globally vs. Thailand



Most serious economic crime experienced by companies – globally vs. Thailand



An interesting outcome of this year's survey is that almost a third (32%) of Thailand respondents expect cybercrime to be the most disruptive economic crime over the next two years, despite just 10% saying that it was the most disruptive over the last two years.

While organisations may be putting this issue at the forefront, past data and other results from this survey indicate that internal threats such as asset misappropriation, procurement fraud, and business misconduct will remain the most prevalent.

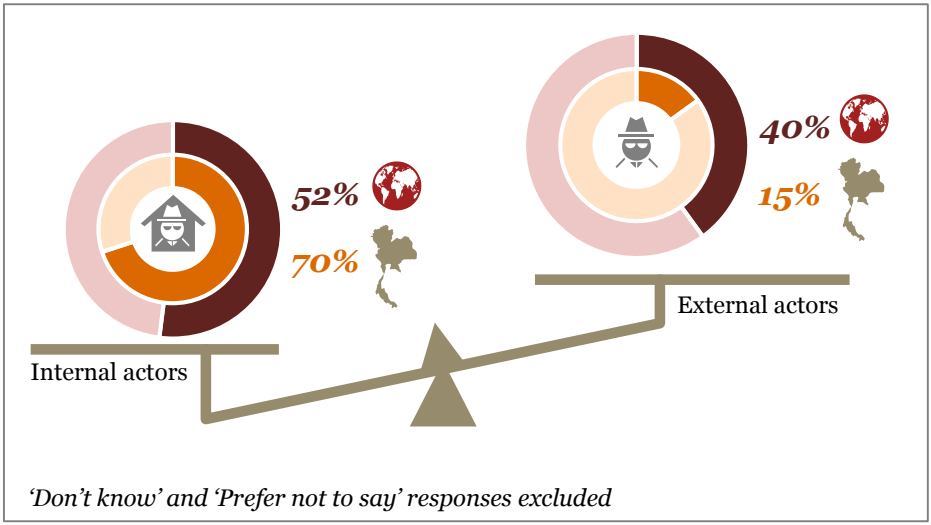
However, cybercrime is a serious emerging threat, and we discuss this further later in this report.

Third party fraud

One of the biggest blind spots that most companies have – and as a result, one of the biggest threats that they face – is from the people that they've invited to do business with them. These third parties include agents, vendors, and shared service providers. It is no surprise that companies naturally expect a certain degree of mutual trust in these business relationships.

Results from the survey suggest that the threat from third parties is below the radar for most companies. Thailand respondents said that external actors were responsible for just 15% of the most serious economic crimes in terms of monetary impact over the last two years. This is less than one quarter of the reported percentage of serious crimes perpetrated by internal actors (70%). Globally, the numbers were much more even, with 52% perpetrated by internal actors and 40% by third parties.

Main perpetrators of the most serious fraud in terms of monetary loss – globally vs. Thailand

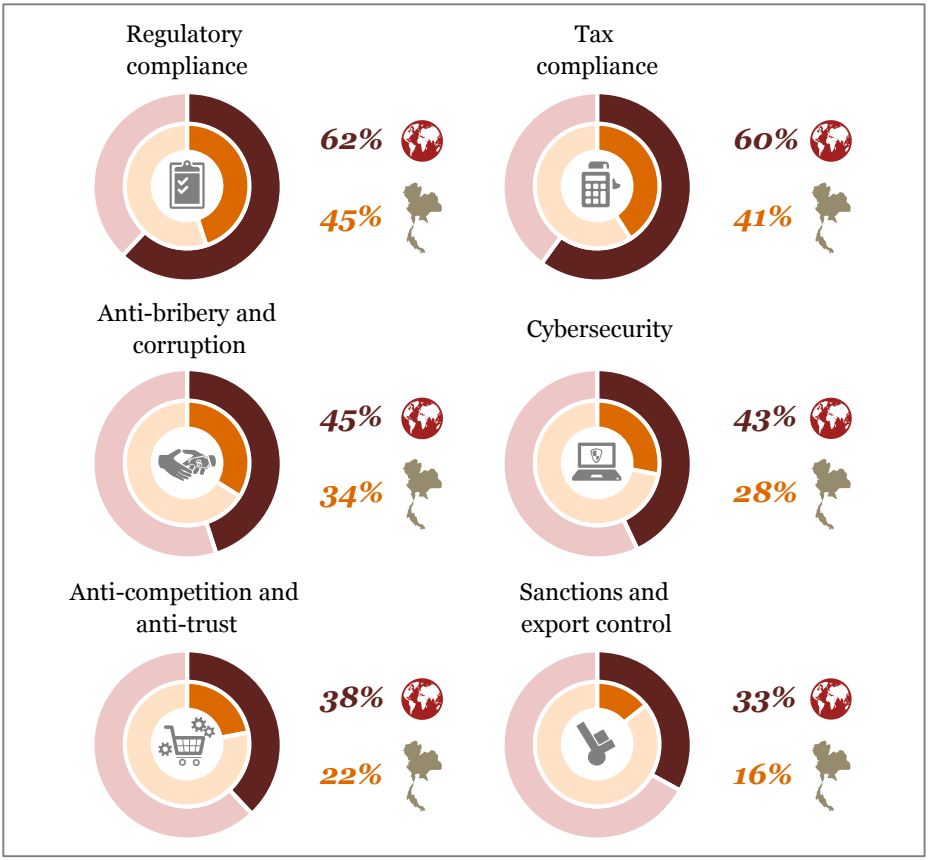


'Don't know' and 'Prefer not to say' responses excluded

Our data doesn't provide a clear explanation for this difference, but a plausible explanation is that Thai companies are better at picking up internal fraud than fraud perpetrated by third parties and customers. Again, it comes back to awareness. It's entirely plausible that a lot of economic crime by external actors goes undetected and unreported.

Our survey didn't ask for information on third party due diligence, but a possible clue into this is the extent to which acquisition due diligence is being done. Thai companies lag significantly behind their global counterparts in this, suggesting they also fall behind on due diligence of their third party such as agents, vendors, and shared service providers.

Acquisition due diligence measures – globally vs. Thailand



As the chart shows, Thai companies are more lax in acquisition due diligence for tax and regulatory compliance, anti-bribery and corruption, anti-competition and anti-trust, and sanctions control than their global counterparts.

Nearly 60% of Thailand respondents hadn't or didn't know if they had completed robust due diligence on target companies in which they are acquiring. Acquisition due diligence is a global norm when considering acquiring a company or entering into a significant business partnership. It helps companies identify irregularities that might be hidden or glossed over and allows them to better assess the risk of the transaction.

Such a due diligence exercise is as critical to an acquiring company as it is to private equity companies. They need to rely on a clean bill of health both for purchasing and selling assets. Sufficient fraud, cyber, and anti-corruption due diligence allows acquirers to know the inherit risks and how to carve them out of the deal, or remediate them post deal. The due diligence results can significantly increase the return on the sale side or the price on the buy side.

Third parties can pose a significant reputation risk. Take for example, the international supermarket chains who have been under fire because of allegations of human rights violations by their Thai partners. The allegations prompted many supermarkets to either stop sourcing from Thailand or to more heavily audit their supply chains.

What can you do?

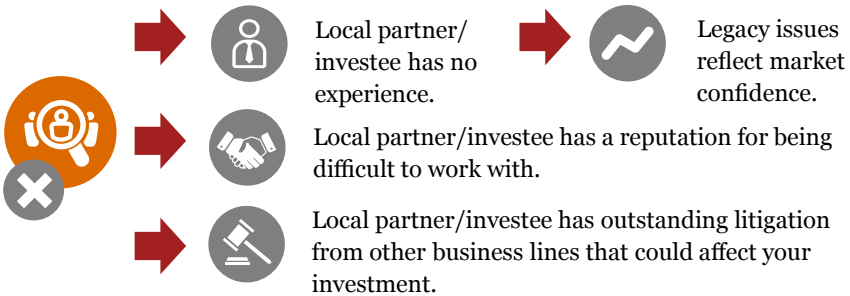
Of the Thailand respondents who conduct due diligence, the majority said that it was focussed on regulatory and tax compliance. However, for due diligence to be of most value, internal corporate parameters need to be considered beyond external compliance.

These are questions we'd like to ask companies to make sure that they're getting the most out of due diligence: *Have you considered reputational due diligence when considering an acquisition? Have you conducted due diligence on your vendors and third parties? Do you know if they pose a risk to your reputation, or if they could be a facilitator for fraud or money laundering?*

And don't forget internal due diligence: *Have you assessed whether your vendors are related to your employees? Have you conducted background checks on your key employees, specifically newly appointed senior management and executives from lateral hire?*

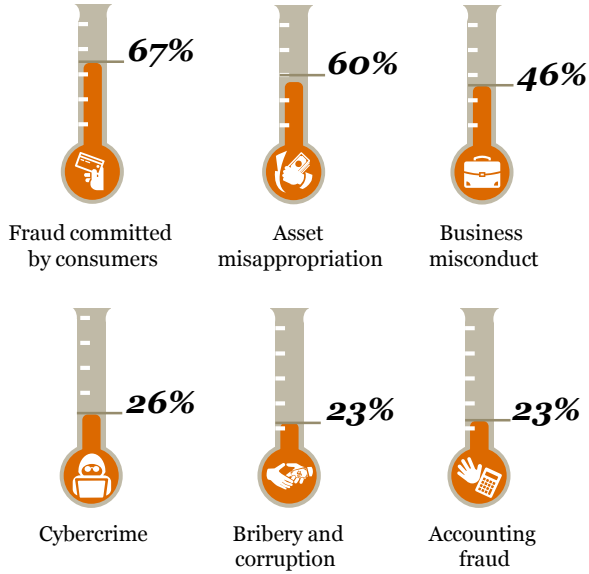
Perhaps your new head of procurement was let go at his last company because he was pushing work at inflated prices to his in-law's company. And perhaps he's doing the same thing now. If you haven't done the due diligence, you're exposing yourself to fraud risk.

Things can go wrong if you haven't done third parties due diligence

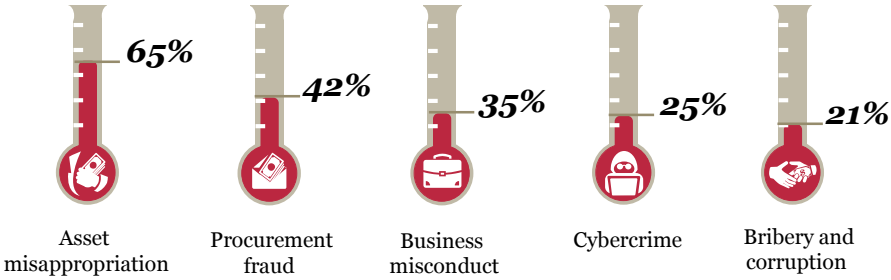


Most common financial services and manufacturing sector fraud experienced by companies in Thailand

Top five types of financial services sector fraud



Top five types of manufacturing sector fraud



Section 3

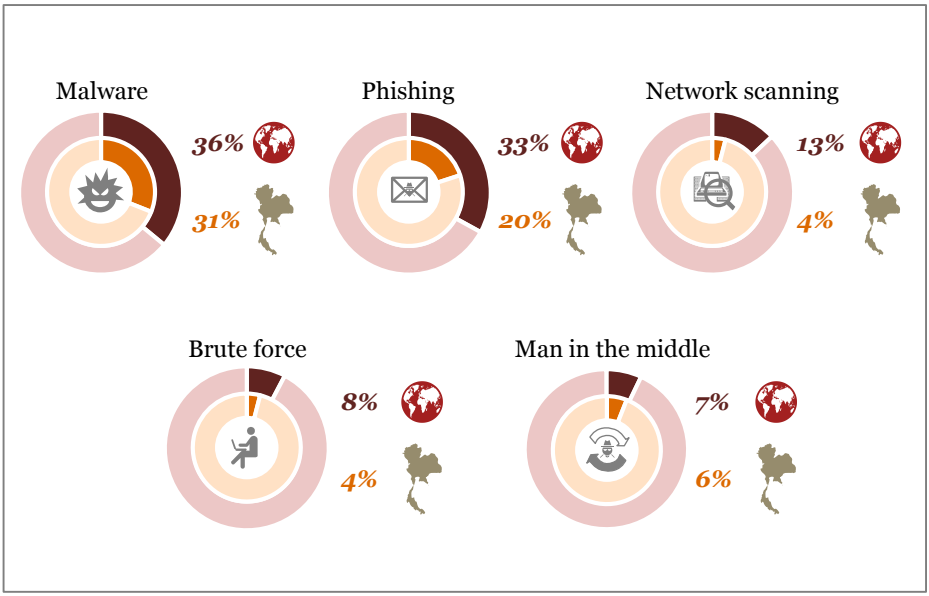
New kid on the block – fear of cybercrime greater than reported attacks, and that's not a bad thing

Just over one in five respondents (21%) said their company had been the victim of cybercrime in the last 24 months, with just over one in ten (11%) ranking it as the most serious in terms of its impact on their organisation. Despite these numbers, almost a third of respondents (32%) predicted that it would be the most serious crime over the next two years.

We believe the discrepancy between past experience and future concerns comes back to awareness of the issue. Cybercrime is the new kid on the block so it's perhaps no surprise that it's on people's minds, especially as Thai businesses transform their operating models to take advantage of online opportunities and make use of emerging digital channels such as cloud solutions in both their front and back office operations.

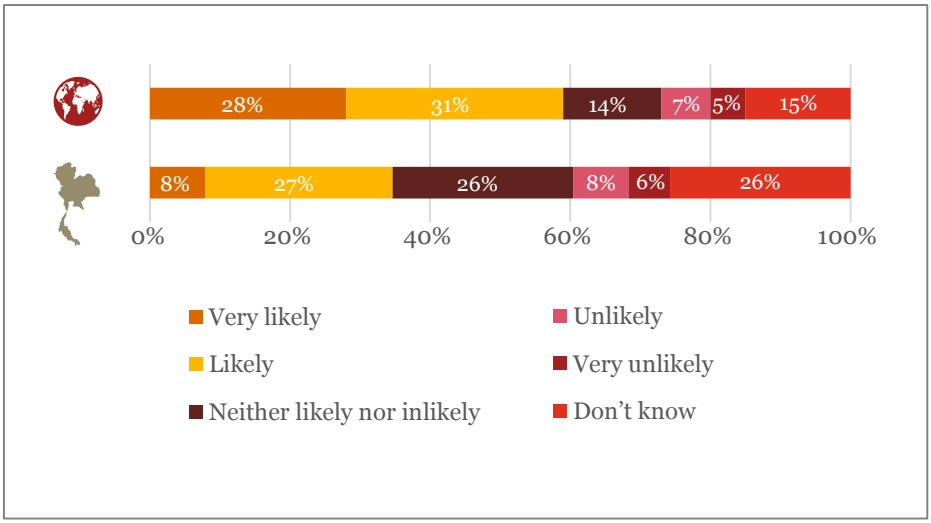
Cybercrime experience and future concerns – globally vs. Thailand

Most reported cyberattacks – globally vs. Thailand



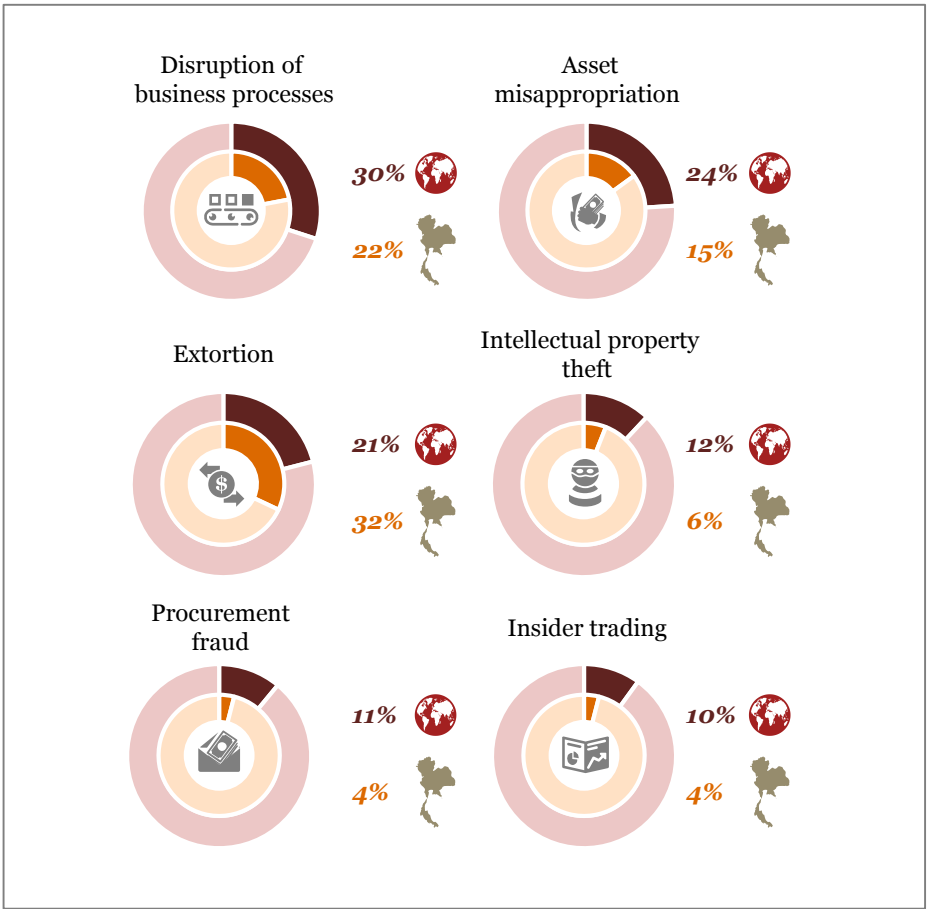
But it is not front of mind for all organisations. Indeed, as noted above, when asked to name what types of economic crime they had been affected by, only 21% of respondents said that they'd experienced cybercrime. However, when asked specifically if they had been targeted by cyberattacks, only 49% said "no" or "don't know". This means just over half of all respondent organisations said that they had been targeted by cyber-criminals, with malware (31%) and phishing emails (20%) being the most prevalent techniques.

Likelihood of sharing cyberattack information with the government or law enforcement – globally vs. Thailand



As with other types of economic crime, we believe that cyberattacks are much more pervasive than the data suggests. The survey response bears this out with only 35% of respondents saying that they're likely or very likely to share information with government or law enforcement agencies about suspicion of or subjection to cyber-attacks, compared with 59% globally. Those who are reluctant to share say it is because they fear that the information would be made public and cause damage to their credibility or reputation.

Fraud and economic crime resulting from a cyberattack – globally vs. Thailand

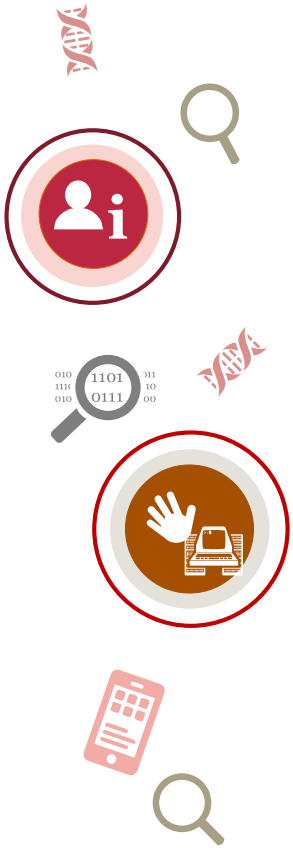


The key characteristics and challenges of today's digital fraud

New digital products are creating new attack surfaces. To bring products to market, companies once followed an established B2B process involving vetted resellers, distributors, and retailers. With today's innovative B2C digital platforms, there is a much wider attack surface – and much more room for fraud to break through.

Industry lines are blurring. In the digital economy, we're witnessing a crossing over of some historical non-financial service companies into payment systems. While financial services traditionally have advanced anti-fraud measures and legacy knowledge to manage fraud and money-laundering risks, some of these relative newcomers to the payment industry lack this experience and know-how – making them, and their third-party ecosystem, susceptible to both fraud and regulatory risk.

The technical sophistication of external fraudsters continues to grow. Cyberattacks continue to get more sophisticated, thorough, and devastating. Consider how a single ransomware attack in 2017 crippled Britain's entire National Health Service (along with hundreds of thousands of computers over the world, including 200 in Thailand), putting lives at risk. Or how, in a 2016 hack, fraudsters managed to subvert banks' SWIFT accounts – the international money transfer system that all banks use to move billions of dollars daily among themselves – stealing nearly US$100 million from the Bangladesh Central Bank.



You can change your credit card number, but you can't change your date of birth. The knowledge-based authentication tools long used to control fraud are outdated, but most companies haven't replaced them yet. When a national entity suffers a massive breach, what's stolen isn't a replaceable asset such as cash – but unique, personal identity markers such as dates of birth or national identification numbers. Since this is the very data that's typically used to verify identity and prevent fraud, a breach like this essentially opens the door for any fraudster to take over a person's identity. Unfortunately, many companies have not yet adopted new techniques – such as digital device IDs and voice biometrics – that are now necessary to protect their customers' assets.

Once fraudsters have cracked your systems, an attack can come at any time. Ongoing security awareness is still the key to preventing cyberattacks, and it's not enough just to be on the lookout for fresh breaches of your systems. One advanced persistent threat (APT) is a type of malware that stays below the radar in corporate IT systems and users' machines to avoid detection and deletion. This allows it to spread and launch continuous attacks without being noticed or wait until the time is right to initiate a major crime, potentially resulting in multi-million-dollar losses.

What can you do?

In Thailand, 61% of respondents said that they use technology as the primary cyberattack monitoring tool, or as part of a wider monitoring programme, although this lags behind the global average of 72%.

Building new capabilities to manage emerging cyber risks is vital to every organisation. This means more than just adopting new technology solutions. It also requires building people's capabilities and embedding processes and clear governance to enable specific risk management. Smaller organisations struggling to resource this adequately should consider outsourcing to professional forensics firms. They can do threat assessments and provide threat management services, including monitoring, detection, response, and remediation. Most importantly, retainer arrangement with a professional forensics firm will help corporation rapidly deploy resources and respond to cyber incident.

Know your cyber risk

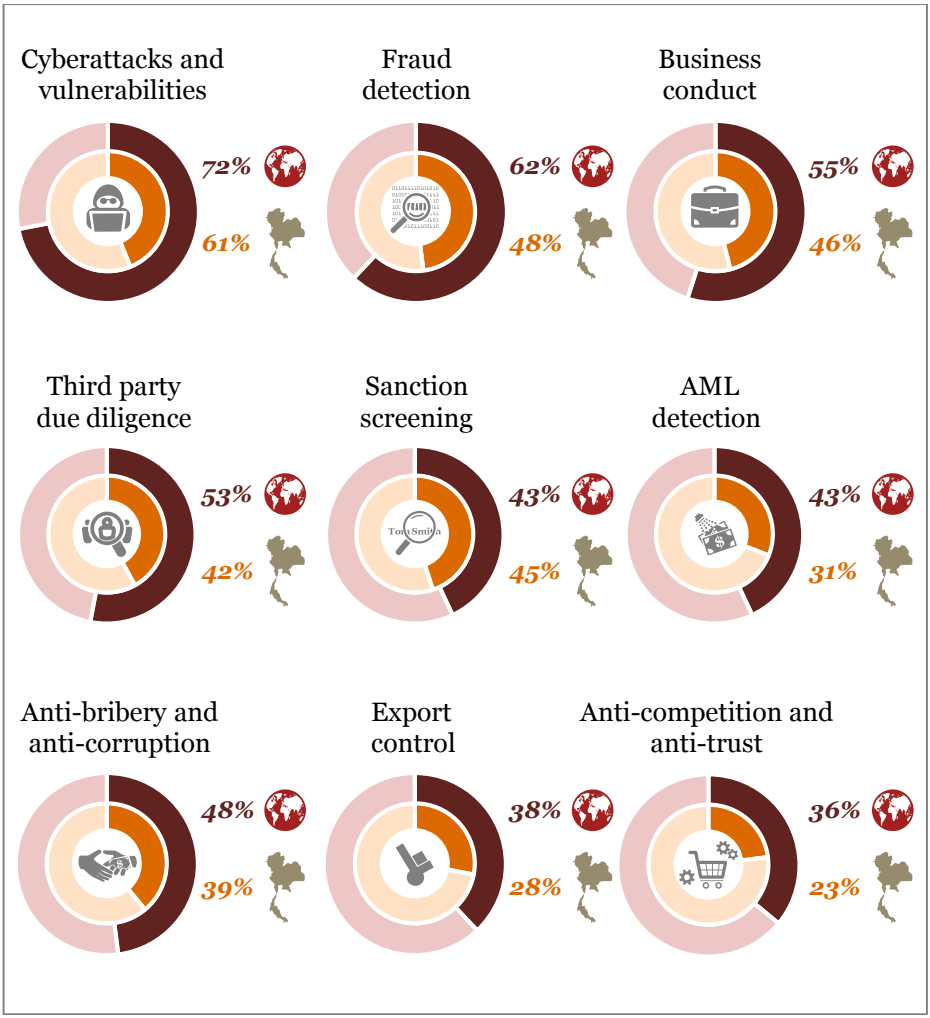
The first step of a robust defence is to conduct an IT cyber risk assessment to check if controls are in place and security is sufficient to prepare for and respond to cyberattacks. A key control for this is a cyber security programme (CSP).

The majority of Thai companies are deficient in this area with only 46% of respondents saying that they have a CSP. While this is up more than half from just 26% in 2016, it's still far behind the global figure of 59%.

Ten percent of Thailand respondents said that they had a CSP but hadn't implemented it, and 16% were assessing the feasibility of implementing one.

Only 7% said that they didn't have a programme, down from 22% in 2016. Although, somewhat alarmingly, 21% didn't know if they had a programme – so we have to assume most of these also do not.

Use of technology as an instrument to monitor fraud and economic crime – globally vs. Thailand



Get your team in place...

...and test how they manage your CSP in a live situation. Simulate an experience that will test how they lead your organisation's reaction to a cyber threat. Ultimately, these scenarios should be documented into a playbook with spectrum of detection, investigation and remediation approaches.

Even with a CSP, without a well-trained and well-led information security manager, companies leave themselves vulnerable to the attack. All it takes is one email with malware to get through security systems, spread through the network, and disrupt business or result in theft of confidential business data.

Only 16% of Thai respondents said that they had a designated Chief Information Security Officer (CISO), less than half the 38% global figure. In our experience, if there is a CISO, they're often not senior management and don't report directly to the board, so their work and results don't get the strategic attention that they need.

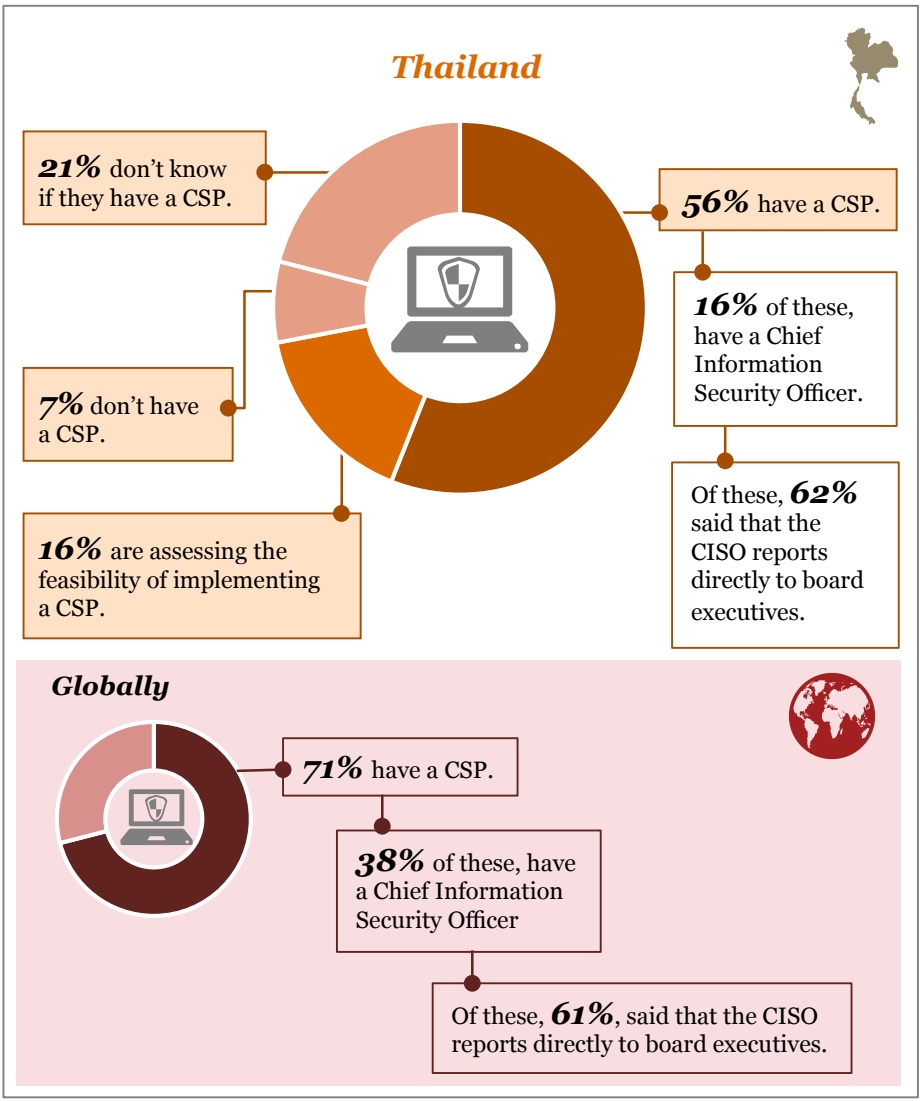
Know how to respond to cyber incidents

A detect-prevent-respond plan should be implemented and regularly tested to limit damage and prevent future attacks. A cyber incident response plan should be in place to ensure that, if an attack does breach defences, loss is minimised and repeat attacks prevented.

Remember the human factor

Lastly but perhaps most importantly, your people are as important to your CSP as processes and technology. From our forensic investigations of cyberattacks in Thailand, we've learnt that attackers frequently get through as a result of human error. Companies should conduct periodic cyber-awareness training for everyone who are using their corporate networks. Cyberattack simulation training for the board and senior management is another reliable way to distill the topic to the leadership and assess the corporate readiness and their understanding of the threats.

How companies prepare to deal with cyberattacks – globally vs. Thailand



Section 4

The fraud triangle – how investment in culture can strengthen your defences against fraud

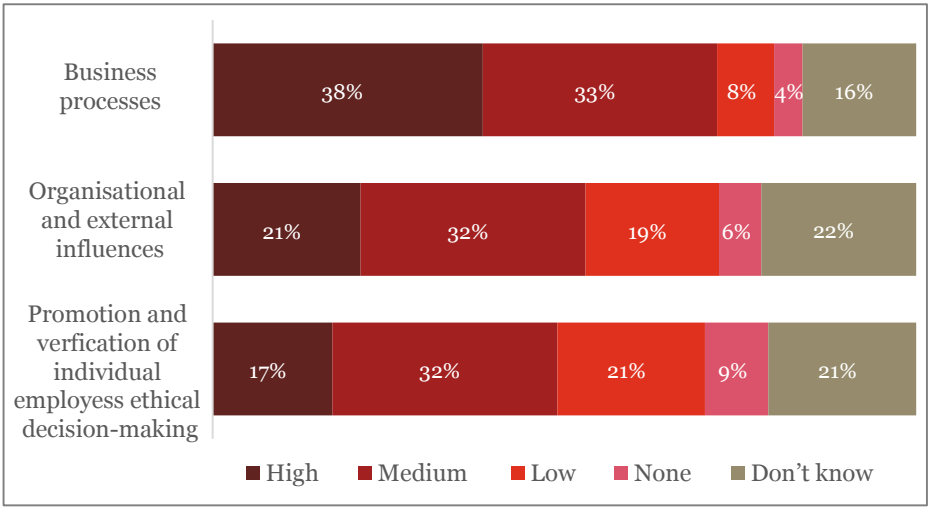
Are you investing where you should to maximise your return?

Growing awareness of economic crime and fraud needs to be accompanied by investment in employees, employee capabilities, and business processes and tools to effectively minimise risk exposure. Responses to the survey show that some companies are doing so, although not nearly as many as we'd like.

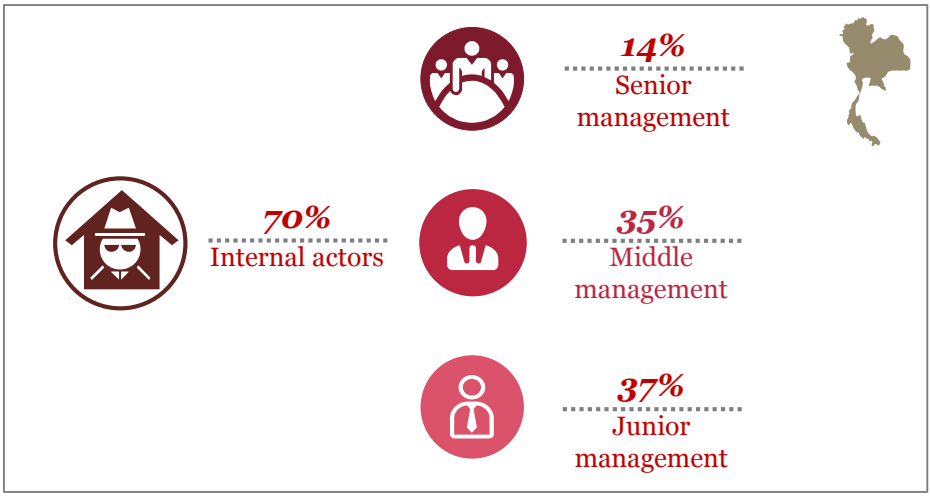
Seven in ten (71%) of Thai respondents said that their companies put medium or high effort into business processes to combat internal fraud and economic crime, compared to 83% globally. However, only 17% said that they put high effort into improving the ethical standards of individual employees, compared to 34% globally.

This is despite 70% of the Thai respondents whose companies had experienced economic crime in the last two years saying that the most serious crime in terms of monetary loss was done by internal actors. Only 15% said that the perpetrator was an external actor.

Effort to combat internal fraud and economic crime



Main perpetrators of the most disruptive fraud in Thailand



Globally, internal and external perpetrators are spread more evenly with 52% of respondents saying that internal actors were responsible for the most disruptive fraud, and 40% saying that external actors did it.

While part of the wider spread in Thailand may be an *awareness* issue – as per the theme of this report – it's clear that Thai companies are susceptible to fraud by employees.

This means investment in human capital to create a zero-tolerance-for-fraud culture should be a priority. As noted earlier, economic crime has a big impact on employee morale. But the flip side to this is that employees can play a big part in prevention if they're supported by the right corporate culture.

It's necessary to invest in people and corporate culture, not just business processes and controls. This requires an understanding of what drives economic crime and fraud. Fraud is the result of a complex mix of conditions and motivations, only some of which can be stopped by business processes.

Fraud incident hinges on people's decision-making, so focussing on human behaviour is the best opportunity to reduce or prevent fraud. The return on investment in people initiatives, such as on ethical decision-making, is likely to far exceed that of investing in more technology to identify or block fraud.

The fraud triangle

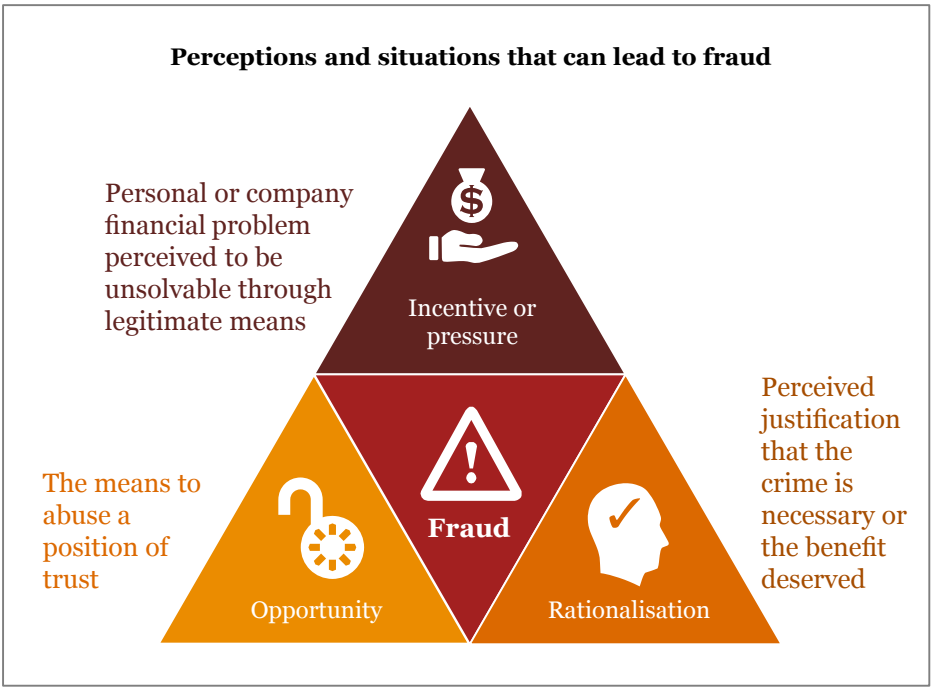
The fraud triangle is a means to understand human behaviour and perceptions that can lead to fraud, and to design ways to mitigate it. The fraud triangle starts with an incentive (generally a pressure to perform within the organisation), followed by an opportunity, and finally a process of internal rationalisation. All three of these drivers must be present for an act of fraud to occur.

Pressure or the incentive to commit fraud is generally stems from a financial issue in an employee's personal or work life, and it may occur at any level of an organisation. At higher levels, it can have its roots in altruism, for instance if an executive cheats to 'save' the company by meeting key financial or other performance targets. In the lower ranks, a sales manager may bend the rules under pressure to meet unrealistic sales expectations. Or an engineer may try to recoup losses after important machinery breaks down because the company has not invested adequately in maintenance.

The motivation may not be money, but fear or embarrassment. In Thai culture, avoiding embarrassment and fear of admitting to a mistake are common. The lies told to cover up the first one often grow in seriousness.

A poorly designed compensation structure may create bitterness among staff and lead to some to try to close the gap through fraud. Some other drivers may be more personal, such as needing to pay high medical bills for a sick relative or to fuel gambling addiction.

Of the three dimensions of the fraud triangle, the bulk of the effort over the last 15 years has gone to addressing the *opportunity* to commit fraud, such as the 71% of respondents who put a medium or high level of effort into business processes such as strengthening internal controls.



But addressing internal fraud requires more than technology and processes, and even well-designed controls can bring a false sense of security that actually exposes a company to greater risk. This is because relying on controls assumes that management will always behave ethically and will rigorously follow standard operating procedures. In fact, experience shows that virtually every significant break down of internal fraud is a result of management circumvention or override of controls. In addition, controls can't overcome collusion, whether it be between employees or, worse, between employees and third parties.

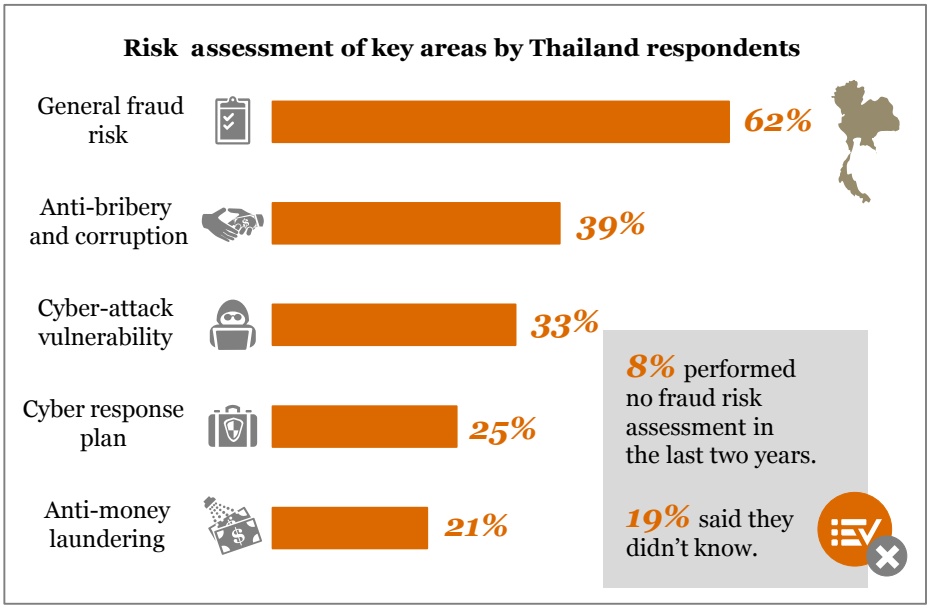
And indeed, our survey reveals that the share of serious internal fraud committed by senior or middle management continues to rise dramatically – up almost half from 34% to 49% since 2016. Addressing this fundamental structural problem requires customising fraud risk controls to your unique business culture and actually planning for possible management override or collusion in targeted areas.

Finally, the fraud triangle requires that the perpetrator finds a way to excuse or *rationalise* their actions, often by finding a way to reconcile it with their own personal code of ethics. They may convince themselves that it is a victimless crime that won't hurt anyone, or that they're doing it for a good reason and that any fall out will be managed before anyone has a chance to find out.

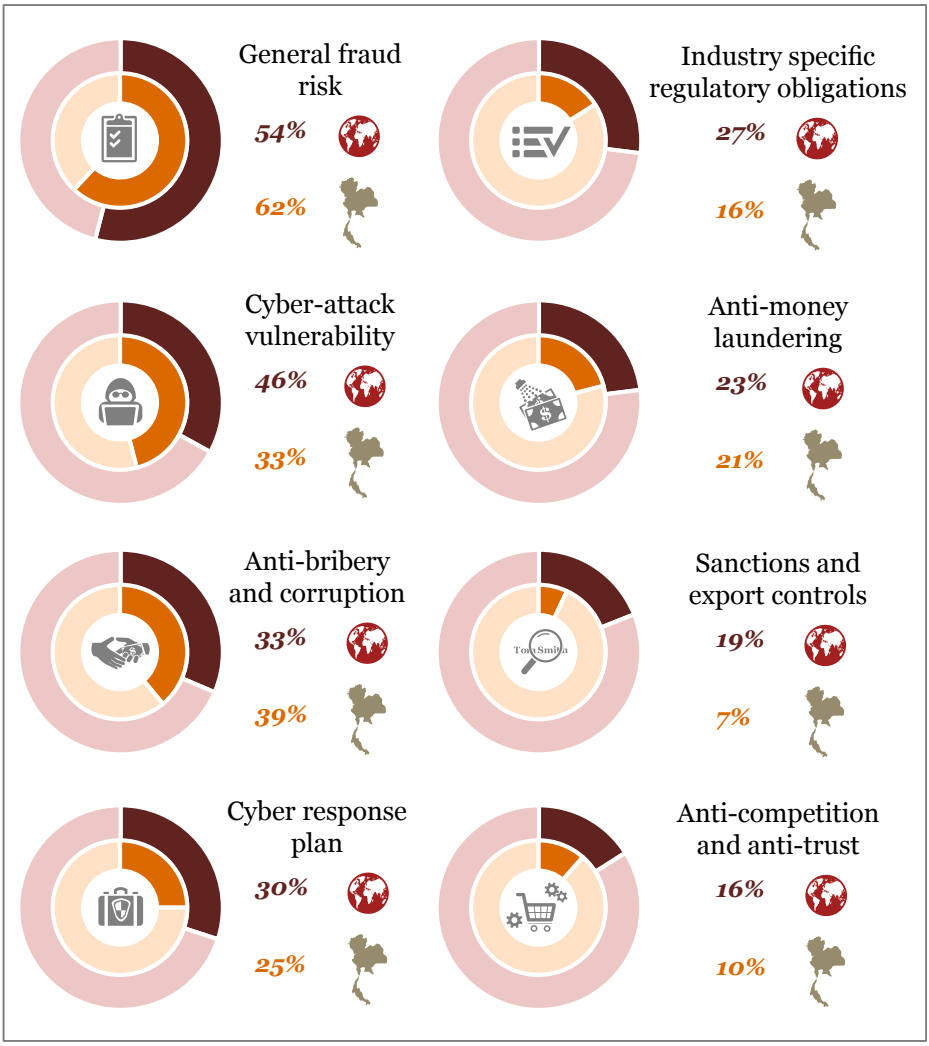
What can you do?

The first step in addressing the fraud triangle is to understand your vulnerabilities through a proactive fraud risk assessment of your organisation. This will help you identify fraud schemes and ensure that the right controls are in place to address the opportunities to commit fraud.

Yet, considering how critical this step is in the fight against fraud, it's astonishing how few companies are taking it. Our survey reveals that over the last two years, only 62% of respondents conducted a general fraud risk assessment, 39% performed risk assessments in the critical areas of anti-bribery and corruption, and 33% assessed their vulnerability to cyberattacks. Only 21% tested their risk for money laundering and a meagre 7% looked into the areas of sanctions and export controls. Almost one in ten respondents (8%) performed no risk assessment in the last two years.



Risk assessment areas – globally vs. Thailand



The next step is to examine the pressures and incentives coming from the top, beyond the expected financial results: *Are these pressures and incentives complying with regulations? Are they consistent with doing the right thing for customers and people? Could over-aggressive sales programmes lead to fraudulent or illegal behaviour?*

Handling the last element of the fraud triangle, *rationalisation*, is where workplace culture becomes critical. But do you really understand your workplace culture, the strengths that you can build on and the weaknesses that might lead to employees rationalising bad behaviour, and acting on opportunities? Often, by recognising operational circumstances deem ambiguous or *gray* and clarifying them in the open.

Start by talking with staff – especially those in positions where they might have the opportunity to avoid or override controls – to understand how internal culture affects them. Support this with workshops and focus groups or anonymous surveys.

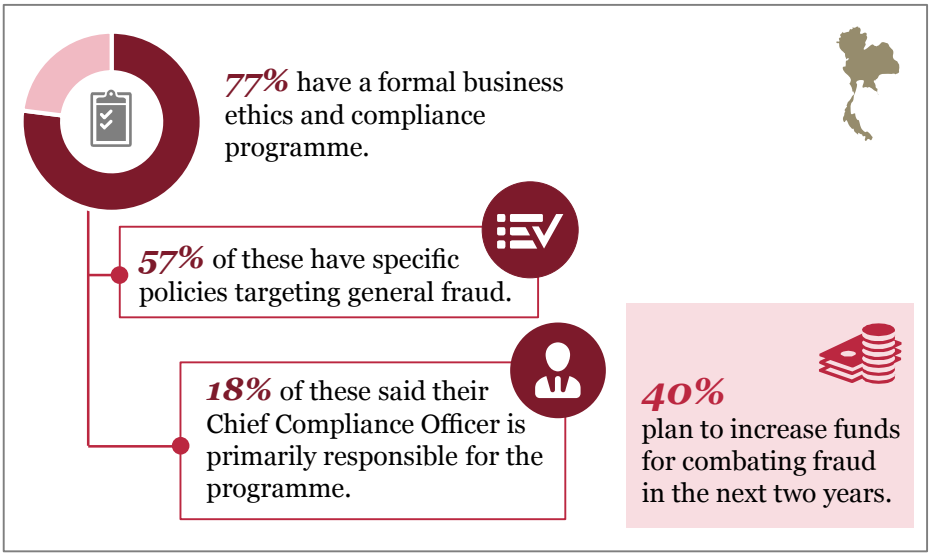
While doing this, make sure that your staff understand what counts as unacceptable behaviour and what the consequences are legally and with how they'll be perceived by colleagues and family if they steal from their employer – and by extension from their co-workers.

Many Thai corporations still don't have a well-defined anti-fraud policy, so the definition of fraud may be ambiguous to some employees. Providing awareness training – and repeating it regularly – will make it that much harder for people to rationalise or justify fraudulent activity. This training needs to be backed up with a well-publicised open-door or hotline policy so staff know who to talk to if they feel pressure or witness others behaving suspiciously.

A good way to drive the message home is to have staff periodically sign compliance agreements confirming that they understand and will adhere to the company's anti-fraud policies. This is especially important in Thailand where things like unofficial 'sales commissions' may be seen as a normal part of entitlement. An official policy will remind management and staff that this is actually fraud. Compliance documents can also serve as an audit trail if needed, and are especially useful for terminations due to a rule breach.

Unfortunately, we've found that most organisations don't invest enough effort in an awareness programme that can make a difference for fraud prevention. In fact, the percentage of respondents who said that they have a formal business ethics and compliance programme dropped from 80% to 77% since 2016. And only 57% of companies with a programme said that their organisation has specific policies targeting general fraud.

Ethics and compliance in Thailand

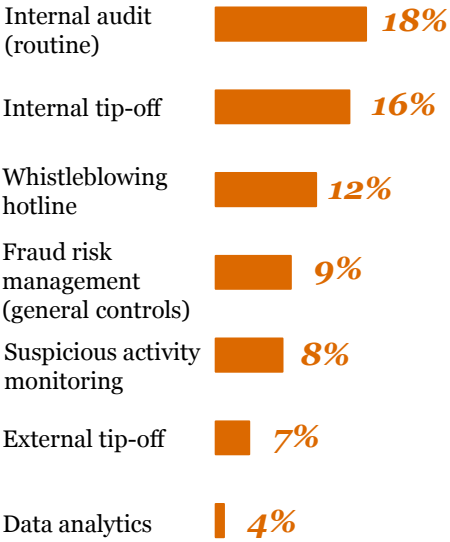


While fraud will always be with us, there are ways to minimise exposure to internal fraud through investing in a culture of zero-tolerance for fraud. Assuming that you already have a well-established control environment, this may offer a surprisingly high return on your investment.

This has been especially true in Thailand, which is already ahead of the curve when it comes to identifying fraud through corporate culture as opposed to corporate controls. Over the last two years, 35% of the most serious crimes were discovered through internal or external tip-offs or from a formal whistleblowing hotline.

Since these channels appear to be working well in Thailand, companies here should continue to enhance them, while also improving internal audit programmes and strengthening other corporate controls.

How the most disruptive fraud or economic crime incident was initially detected – Thailand



Top 6 most serious economic crimes – Thailand

Takeaway questions

Have you completed a fraud risk assessment recently? If not, why not?

Do you know the norms for ethics and compliance in your industry?

Does your ethics and compliance programme explicitly target fraud?

Do your incentives and pressures comply with regulations? Are they consistent with doing the right thing for your customers and your people?

Do you have an open-door policy or hotline that could deliver early-warning signs of internal fraud?

Have you looked at your workplace culture to identify potential trouble spots?

Section 5

Technology – an opportunity for enhanced fraud prevention

There is hardly a single business process that hasn't changed drastically over the last decades due to the integration of technology. But just as it makes business processes quicker and easier, technology is a double-edged sword that also makes it easier for fraudsters to commit and hide crimes.

On the plus side, using technology for crime leaves evidence that can be picked up by companies with the appropriate fraud fighting technology.

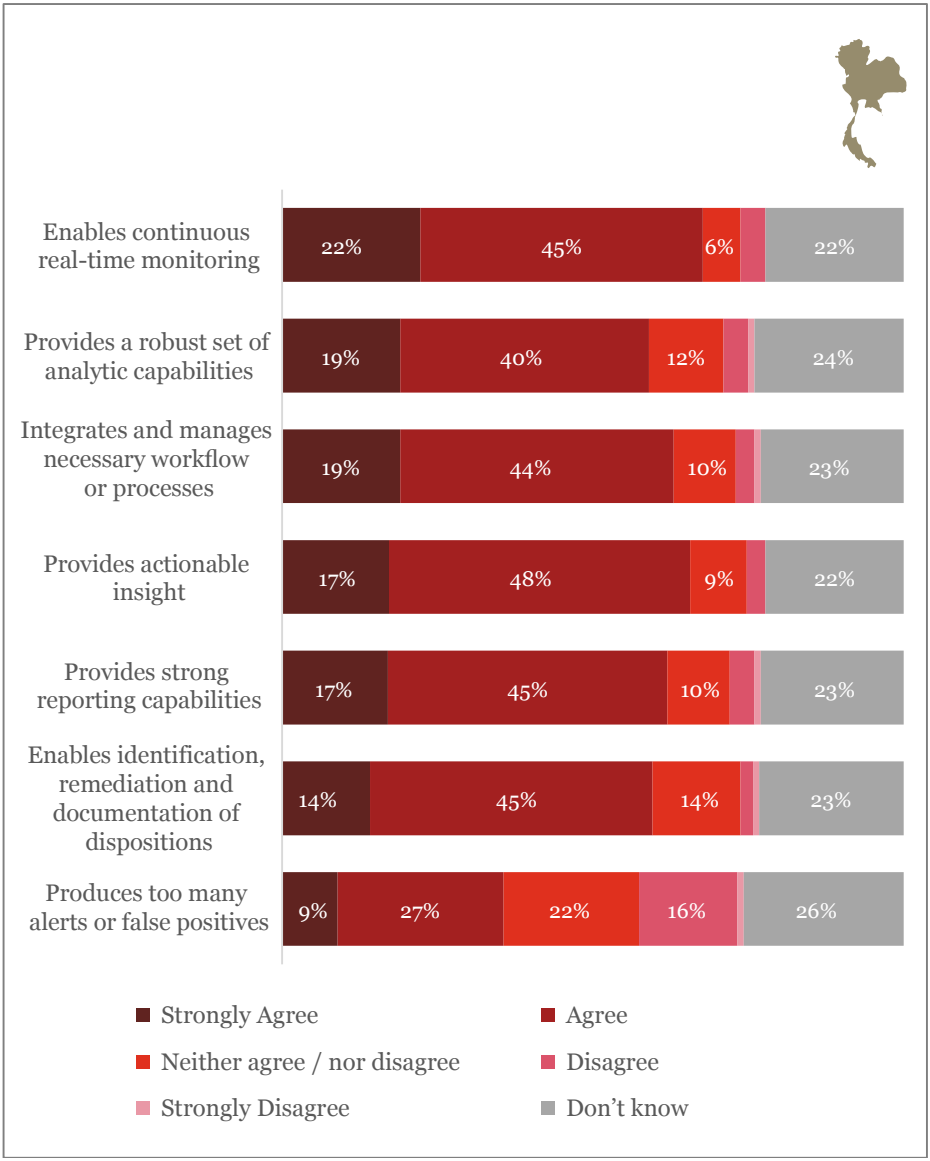
On this front, there is a wealth of innovative and sophisticated technologies available. However, in Thailand, 48% of respondents said that they use technology as the primary technique for monitoring of fraud, and 39% use technology to monitor bribery and corruption.

While most Thailand respondents agreed that using new technologies could enhance their fraud prevention and detection processes, 50% didn't use technology at all or didn't know whether their organisations used technology to detect fraud or cyberattacks, or to conduct third party due diligence.

The effectiveness of the technology used is also a crucial point to consider. Our survey revealed a disconnect with understanding the most appropriate and effective places to invest. For instance, more than a quarter (27%) of Thailand respondents said the system or tool that they used for fraud detection generated too many false positives. This can erode confidence in fraud screening capability, and perhaps cause people to ignore alerts triggered by a criminal act.

This makes it critical for organisations to ensure they've deployed their technology correctly and their teams have the right knowledge to manage it to the best effect.

Attitudes of Thai companies towards using technology to combat fraud and economic crime



Our experience in Thailand has taught us that continuous auditing or monitoring systems have to work in tandem with a continuous feedback systems so that they can learn to differentiate true hits from false positives. The ability to quickly customise an algorithm or risk indicator is crucial to the ability to adapt to emerging fraud schemes. This assumes that the baseline detection rules have already been refined and monitor the risks identified from a proper fraud risk assessment. Eventually, the feedback gathered can be used in predictive modelling and artificial intelligence to apply more advanced analytics to combat fraud by recognising pattern based on historical events.

It's clear that Thai companies have ground to make up. But technology is expensive to buy and adopt across a large organisation – prohibitively so, for some. And decisions on whether to custom develop one or what to purchase, and when, is a delicate one. Some organisations invest in emerging or disruptive technologies but don't use them optimally. Others jump in too late and find themselves behind the curve in the struggle to catch fraud or flag potential trouble spots.

The ubiquity of technology and the stealthy growth of fraud are creating a double challenge for all organisations: finding the right balance between effectiveness and cost, while also keeping pace with fraudsters who are constantly evolving their mode of attack.

Section 6
Conclusion

Be prepared. Face the fraud. Emerge stronger.

Economic crime and fraud are very real threats that all companies in Thailand face. The best way to address them is with eyes wide open and by shining a spotlight into every corner of your organisation to find where fraudsters are lurking ready to attack.

Our survey shows that many companies are under prepared to face fraud. And their weakest areas are also where they could find significant opportunities if the necessary changes are made. Not least of which is creating a workplace culture that is positive and attuned to the needs of the business. This can make a company stronger and more strategic, in good times and bad.

The value of an up-to-date anti-fraud programme can be difficult to quantify, and therefore to free up the necessary investment. But the cost of doing nothing and suffering an attack can be significant from financial, legal, regulatory, and reputational perspectives.

Contact

Vorapong Sutanont
Partner
Forensic Services, PwC Thailand
Tel: +66 (0) 2844 1000
Email: vorapong.sutanont@th.pwc.com

www.pwc.com/th