Economic crime in Thailand

pwc

www.pwc.com/crimesurvey

Contents

Foreword

Economic crime remains a serious issue affecting Thai organisations.

This unfortunate fact rings true time and time again. Our 2016 Thailand Economic Crime Survey shows how fraud continues to victimise responsible businesses and the greater public.

As in previous years, our survey's aim is to inform business leaders, policymakers and the public about developments in the increasingly complicated threat landscape in Thailand – long considered a medium-to-high risk country for economic crime.

Our 2016 survey shows that economic crime is still a serious concern for Thai companies. Four in ten listed firms experienced fraud.

Nearly 80% of incidents of wrongdoing stemmed from within organisations, compared with 46% globally.

Asset misappropriation, cybercrime, bribery and corruption were the most common fraud types in Thailand. Meanwhile, other crimes such as procurement fraud and anti-money laundering span industry sectors, causing financial losses. These critically damage morale and a company's reputation.

Despite greater efforts by the public and private sectors to combat ever-evolving fraud risks, businesses must map out a viable plan to equip their people, set up processes, and invest in technology that bolsters their capability to fight this challenge.

I'd like to express our sincere appreciation to those that participated in the survey, including the partners and staff who contributed to making this report.

I hope that this survey will help you in your ongoing endeavours to curb economic crime.

pwc

Sira Intarakumthornchai
Chief Executive Officer, PwC Thailand

Foreword

PwC's Economic Crime Survey in Thailand has been a great success with a record number of participants; more than 250 companies with nearly half being C-suite respondents.

The high response rate shows that Thai companies are waking up to the reality that fraud poses a growing risk. The number of fraud cases continues to rise, and our survey found that lax detection mechanisms play a key role. For example, within SE Asia, Thailand lags behind in creating an employee speak-up culture – an important early fraud-detection mechanism. Inadequate whistleblowing programmes impede red flag detection allowing fraud to flourish on the work floor.

Cybercrime continues to threaten Thai companies – especially in the financial services sector. For both banks and their customers, fraudsters from Thailand and abroad are exploiting the growing online banking and e-commerce services. Banks are under unprecedented pressure to generate growth in a slow finance market; often causing them to trim spending on their anti-fraud programmes. Although such measures reduce costs in the short term, they can contribute to massive security breaches down the line.

I hope you'll find the information provided in this report insightful in strengthening your ability to combat fraud.

pwc

Vorapong Sutanont
Partner
Forensic services, PwC Thailand

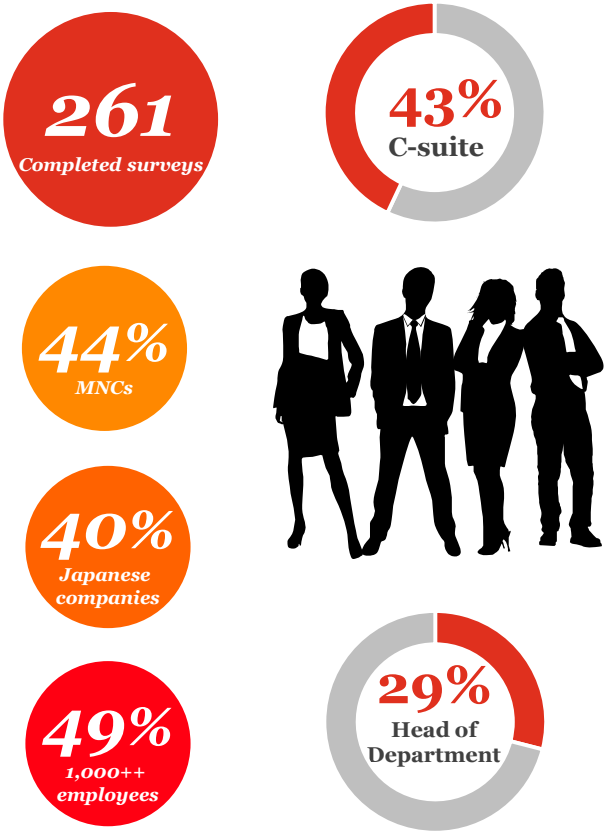
In Thailand, four in ten listed companies experienced fraud.

Economic Crime in Thailand

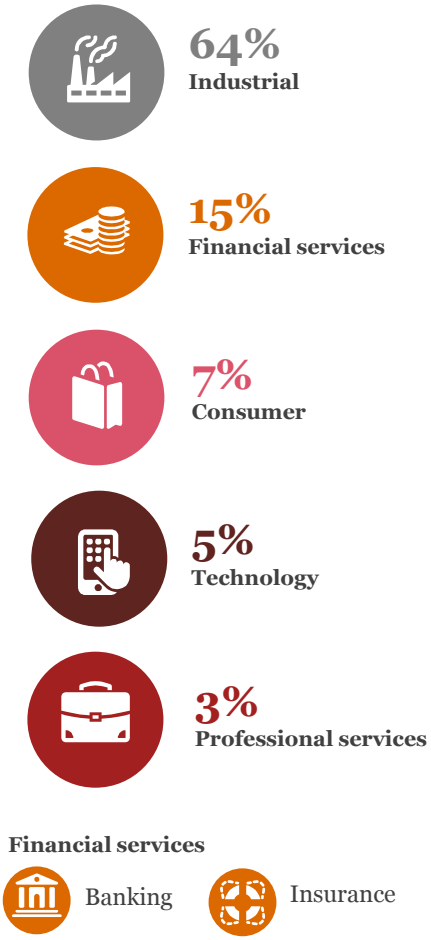
Thailand's part in PwC's *2016 Global Economic Crime Survey* (GECS) garnered the most responses from senior decision makers, with 261 participants completing the survey compared to 76 from the past report. Respondents were from a wide range of sectors representing a mix of listed, private and public sectors. The C-suite made up 43% of the respondents, and another 9% were senior vice presidents, vice presidents, and directors.

Of the total respondents, 44% were multinational corporations, 40% represented Japanese companies, and 49% were companies with more than 1,000 employees. The largest number of respondents were from the manufacturing sector, followed by automotive and financial services.

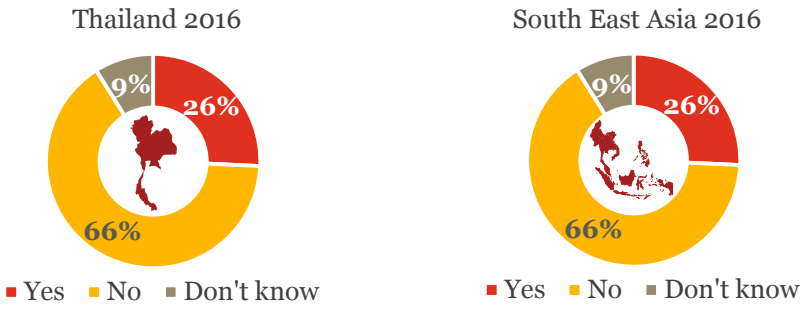
Participation statistics



Industry sectors

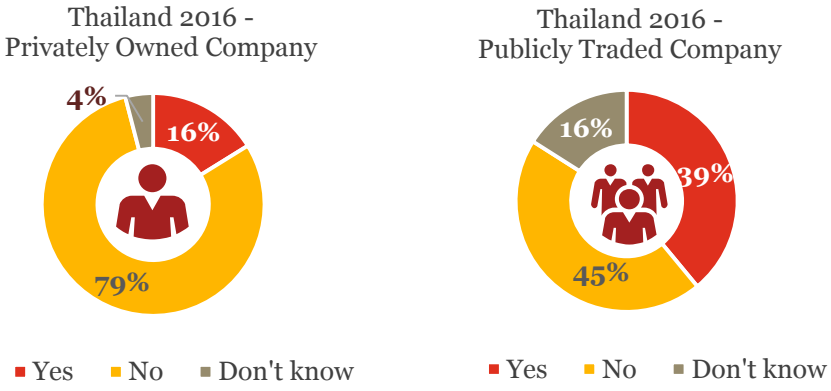


Percentage of organisations in Thailand who experienced economic crime in 2014 and 2015



The latest survey found that although Thailand's overall fraud rates are in line with South East Asia's average of 26%, many organisations admitted that the numbers could be higher as they were uncertain if their existing systems were able to detect fraud.

Private vs. listed Thai companies who experienced economic crime in 2014 and 2015



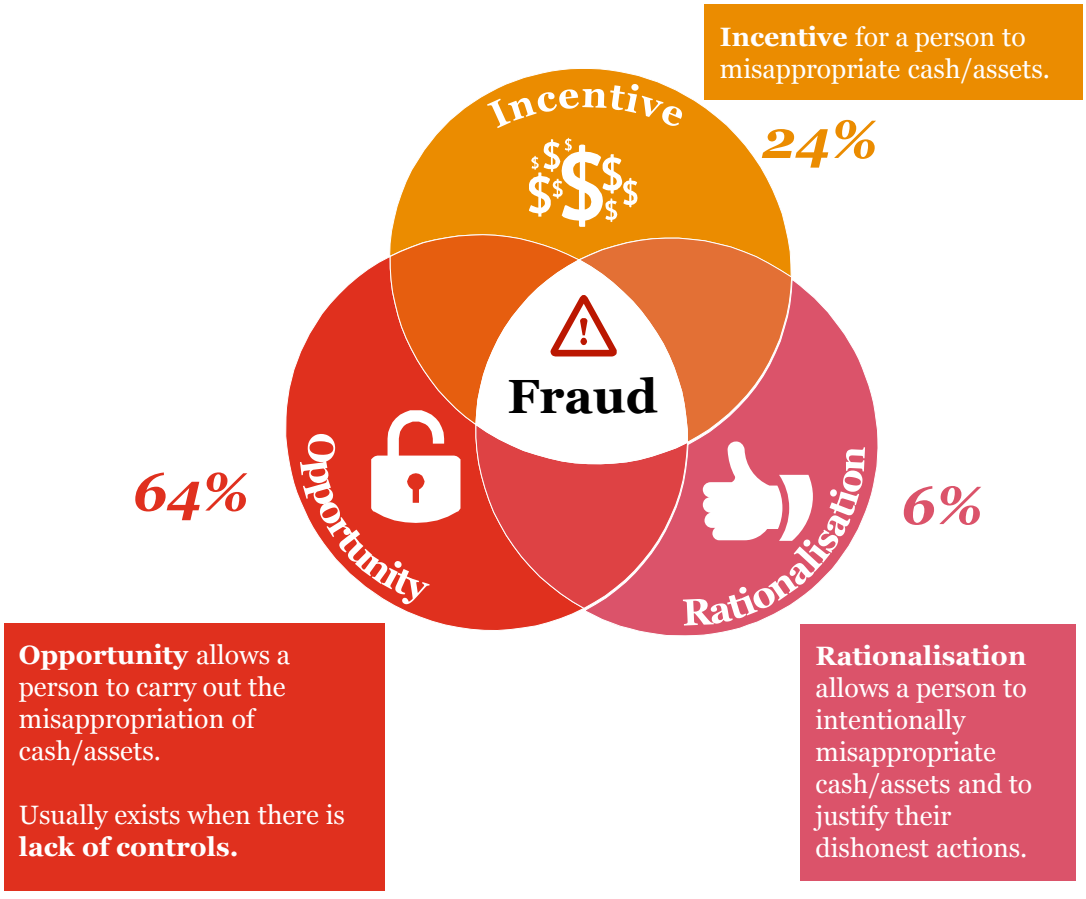
In Thailand, 39% of listed companies experienced fraud as did another 16% of private companies, which is below the global average of 30%. A number of initiatives have been developed in the past few years to help Thai companies prevent fraud, including capacity-building initiatives by the Economic Crimes Suppression Division of the Royal Thai Police, and non-binding recommendations from private sector bodies such as the Collective Action Coalition (CAC) by the Thai Institute of Directors (IOD).

Globally, more economic crime was reported at publicly traded companies (41%) than private entities (30%). Four-in-ten (43%) mid-size or larger companies reported fraud, compared to three out of ten small companies with fewer than 1,000 employees. Half the financial services respondents (48%) said that fraud was found in their organisation, while just 33% in other sectors said that they had suffered from fraud.

Almost 80% of incidents of serious economic crime were perpetrated internally, which is considered high risk because employee fraud is more difficult to detect.

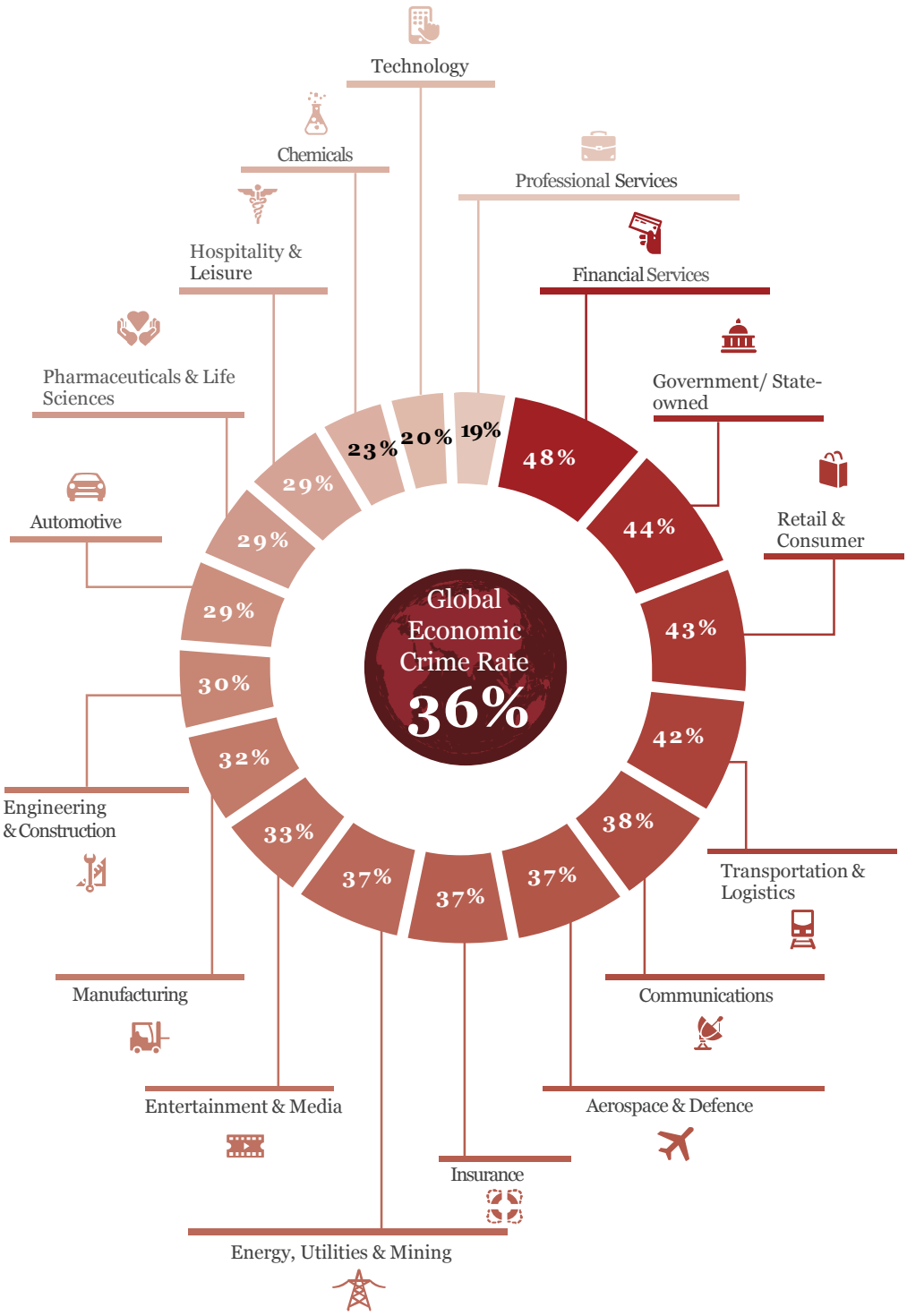
In line with global and regional trends, most respondents (64%) said that internal fraudsters are motivated primarily by opportunity, or the ability to commit fraud. This finding reinforces the need to have strong internal controls and anti-fraud measures as deterrents. Employee morale also plays a role in fraud risk because disgruntled staff are more likely to cheat their employers.

Perceived factors that contribute to fraud



Global view

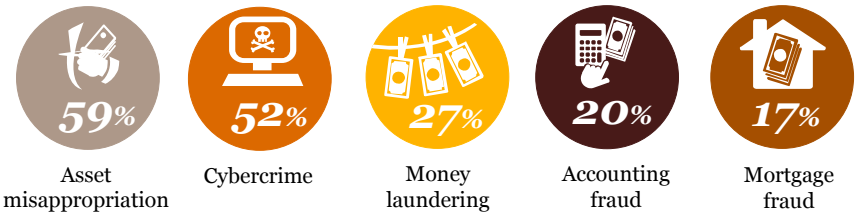
Which industries are at risk?



Globally, 2,251 companies that were surveyed had suffered from economic crime. Financial services has traditionally been the most susceptible to economic crime. But with more companies offering in-house financial services and products, many traditionally non-financial organisations are seeing a concurrent rise in fraud. Businesses in the automotive, retail and communications sectors, to name but a few, are either in joint arrangements with financial services companies or have banking licences. Fraudsters seeking to follow the cash now have more avenues than ever before.

While the financial services industry, by virtue of its highly regulated environment, has built up sophisticated controls and anti-fraud mechanisms over the past decades, the hybrids have yet to come into their own in managing risks in the fast evolving compliance landscape in which they now find themselves. We explore this area further in the anti-money laundering section.

Top five types of fraud in the FS sector



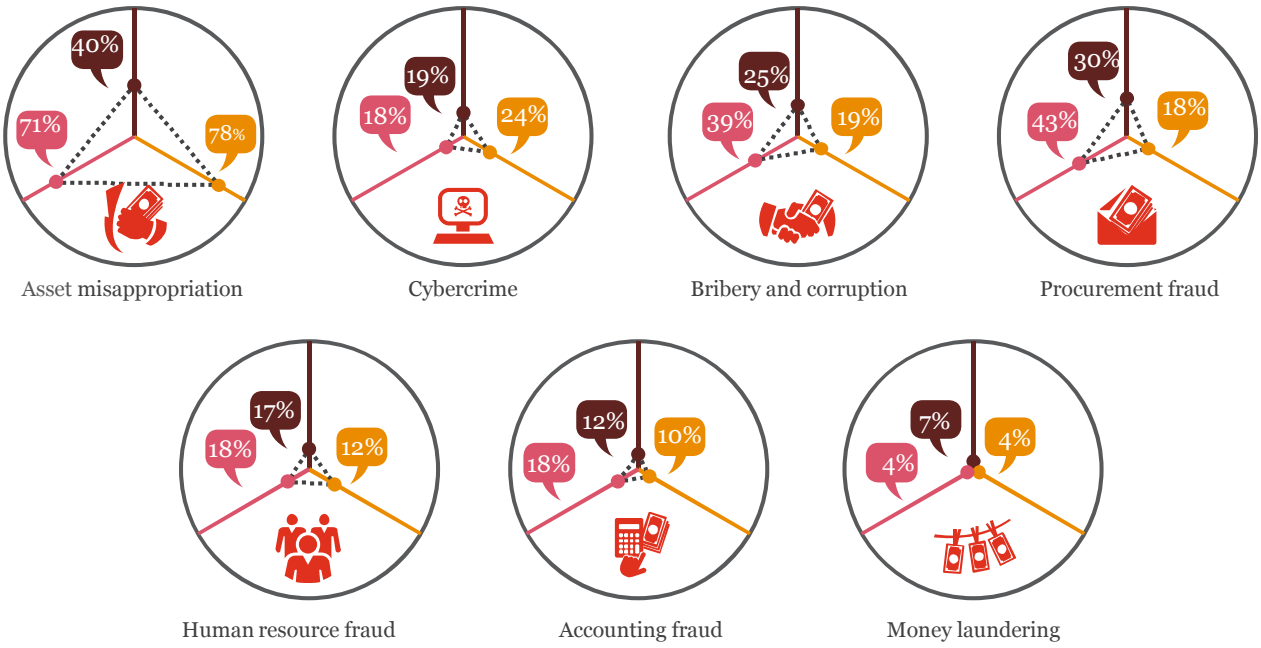
Top five types of fraud in the non-FS sector

The global results show that the five biggest economic crimes for non-financial services companies are asset misappropriation, bribery and corruption, procurement fraud, cybercrime and accounting fraud. While the biggest economic crimes for financial services companies are asset misappropriation, cybercrime, money laundering, and accounting fraud.

The survey findings also suggest that governance, risk and compliance technology reduces corruption and fraud risk. PwC's 2015 State of Compliance survey found that many financial institutions (28%) have begun to use GRC technology to manage risk – from automating compliance tracking and suspicious transaction monitoring, integrating internal audit processes to high-risk areas flagged by the risk management departments.

The seven most pervasive economic crimes reported by our respondents over the two-year survey period

Thailand 2014 vs. Thailand 2016 – All sectors



Asset misappropriation

Asset misappropriation remains Thailand's most common economic crime at 78%, above the 64% global average and the South East Asia average of 69%. Alarmingly, in the past two years, half of the incidents reported by companies in South East Asia occurred in Thailand. In our previous survey, respondents said they expected asset misappropriation would remain a top problem. However, the current survey shows that fewer organisations, only four in ten, had this expectation for 2016 and 2017.

Cybercrime

This is Thailand's second most common economic crime. A quarter of respondents said they'd experienced cybercrime, which is in line with figures reported globally (32%). From our forensics investigations in Thailand, we've seen a significant increase in cybercrime since 2011. While 19% of respondents expect only a few of cybercrime cases in the next few years, organisations in Thailand should not downplay its risk, prevalence or likelihood.

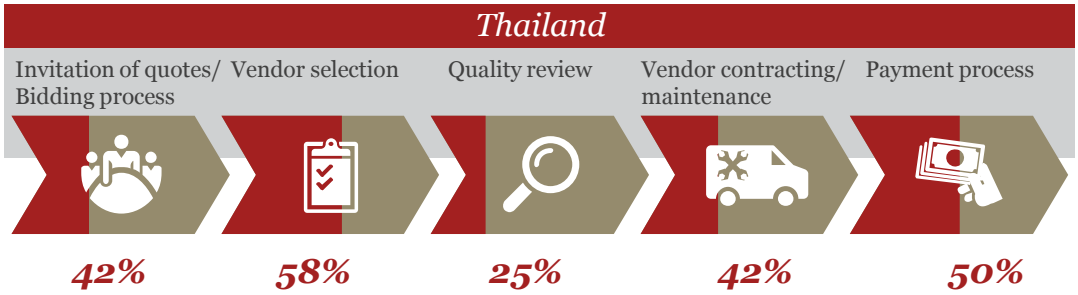
Bribery and corruption

Thailand's bribery and corruption rate fell 20% in the survey period, with only 19% of respondents reporting corruption compared to 39% in 2014 and 54% in 2011. For the following two years, one-quarter of Thai companies believe that bribery and corruption is likely to occur in their organisation, while another 23% were not sure whether their organisations are corruption free. So in effect, close to half of organisations in Thailand felt that they had substantial bribery and corruption risk.

The current Thailand administration has enacted measures aimed at combatting corruption, including the establishment of a criminal court for state officials and separate regional courts for provincial corruption matters. The government has also announced that, by the end of 2016, the Council of State will pass an executive decree to address corruption. Other state bodies are in place to investigate and report on corruption, including the National Anti-Corruption Commission. This Commission previously published a report of the assets of Thailand's top government officials. The effectiveness of these bodies is subject to debate in the media, business circles and international corruption watchdogs.

In 2010, Thailand's Private Sector Collective Action Coalition against Corruption was founded to create greater awareness of fraud risk and implement effective anti-corruption policies and mechanisms to prevent corruption in private companies and industry. So far, 548 companies including 316 listed ones have joined the CAC network. Of these, 152 firms are certified and another 396 are working toward certification as of March 2016. Future economic crime surveys may shed light on the success of local anti-corruption bodies and initiatives in combatting Thailand's prevalent fraud and bribery problems.

Procurement fraud



Procurement fraud

Procurement fraud in Thailand fell below the global average. Our previous survey found that almost half (48%) of Thai companies had experienced procurement fraud during quote and bid solicitation (67%) and vendor selection (58%). To prevent these areas of procurement fraud, we've been recommending that companies strengthen their vendor selection criteria and perform background checks and due diligence on prospective vendors. Adoption of these measures by Thai organisations could be a factor in the significant drop in procurement fraud in the past years.

This year's survey results show that most procurement fraud in Thailand – nearly 60% – now occurs during the vendor selection process. We've also seen a significant rise in fraud during the payment process, from 25% in 2014 to 50% in 2016. Increasing Internet banking channels for payment could be a factor as they offer more possibilities for exploitable vulnerabilities. We found that these emerging service channels still lack adequate internal controls and proper verification methods.

More procurement fraud has also occurred during the vendor contracting and maintenance process (42%) than was found in the 2014 study. Therefore, Thailand companies should strengthen the internal controls from quote solicitation through payment processes.

Human resources fraud

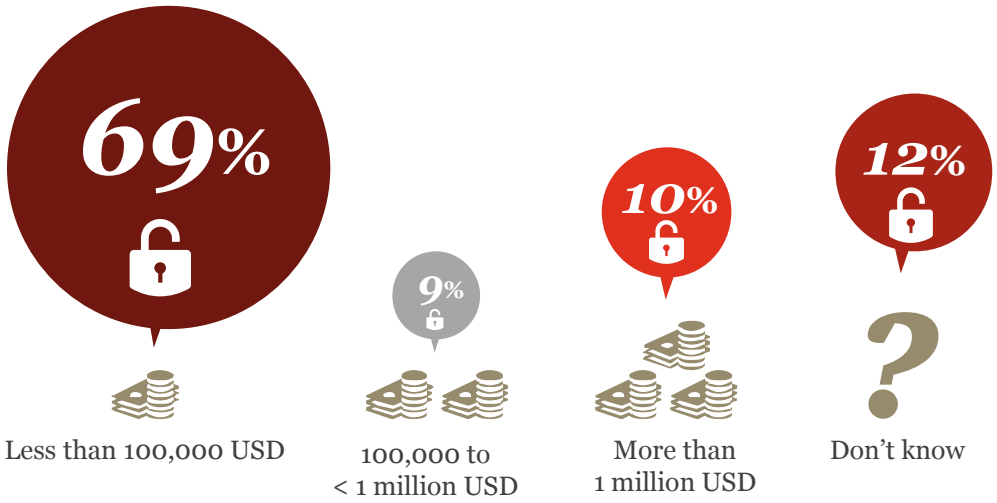
Nearly twenty percent (17%) of respondents are concerned about human resources fraud risk, which includes recruitment and payroll fraud. Our survey found that the most prevalent types are 'ghost employees', which is putting fictitious people on the payroll to take an extra salary, and false qualifications (38% each). Paying ghost employees and hiring based on false qualifications can cripple a business financially and erodes trust. For this, preventive internal controls are an important first line of defence to halt the recruitment of future fraudsters.

Our experience into this line of fraud suggests that the management should conduct pre-employment background screening for mid-management and senior management candidates as well as implementing effective internal practices to prevent ghost employees. HR departments should take an active role in preventing defrauders from simply leaving the company and securing work at another company, which is fairly common in Thailand.

Accounting fraud

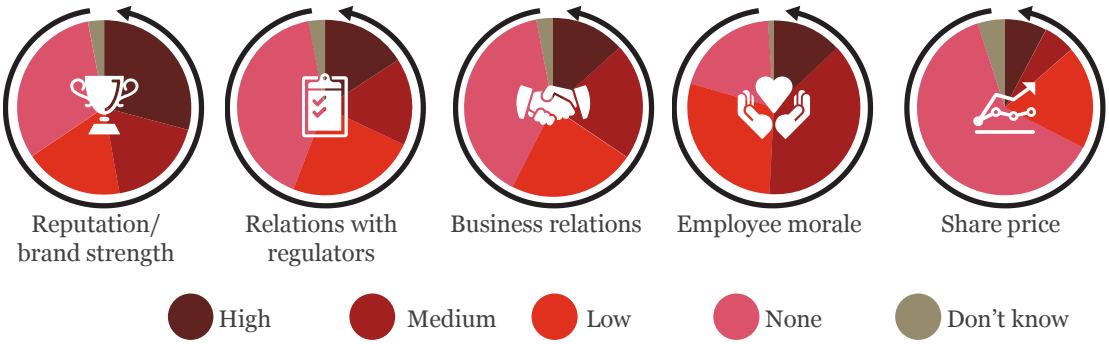
Accounting fraud may be more prevalent than the survey results suggest. In Thailand, it mainly involves making fraudulent transactions and avoiding detection by manipulating financial records, so it is often classified as part of other types of fraud, such as asset misappropriation and procurement fraud.

Financial damage caused by economic crime in 2014 and 2015



Seven in ten (69%) Thai companies reported losses of less than $100,000 (approximately 3.5 million baht) to economic crime over the last two years and just 9% of respondents experienced losses of between $100,000 and $1 million (approximately 3.5 and 35 million baht). Ten percent of respondents reported losses in excesses of $1 million (approximately 35 million baht). In other words, almost one-quarter of Thai companies have lost more than $100,000, (approximately 3.5 million baht) to fraud.

Non-financial damage caused by economic crime in 2014 and 2015



Our survey measured the non-financial impact of economic crime that included harm to reputation and brand strength; and damage to employee morale. Economic crime also affects relations with regulators, business associates and employees. Ultimately, fraud may impact revenue and business growth long after cases are resolved.

Our respondents told us that the greatest organisational damage that they experienced as a result of economic crime was not found in their share price or even in relations with regulators. It was reflected in the damage to employee morale, with 50% citing a medium to high impact, and reputation, with 47%. In both cases, the nature of how a business is *perceived* — from the inside as well as the outside — was the area of greatest concern. This underscores the key role played by values in a successful business strategy.

To prevent fraud, we suggest implementing comprehensive anti-fraud programmes and roadmaps covering policies, fraud response plans, fraud risk assessments, communications, fraud awareness and internal controls training and fraud risk monitoring.

Organisations in Thailand should not downplay cybercrime risk, prevalence or likelihood.

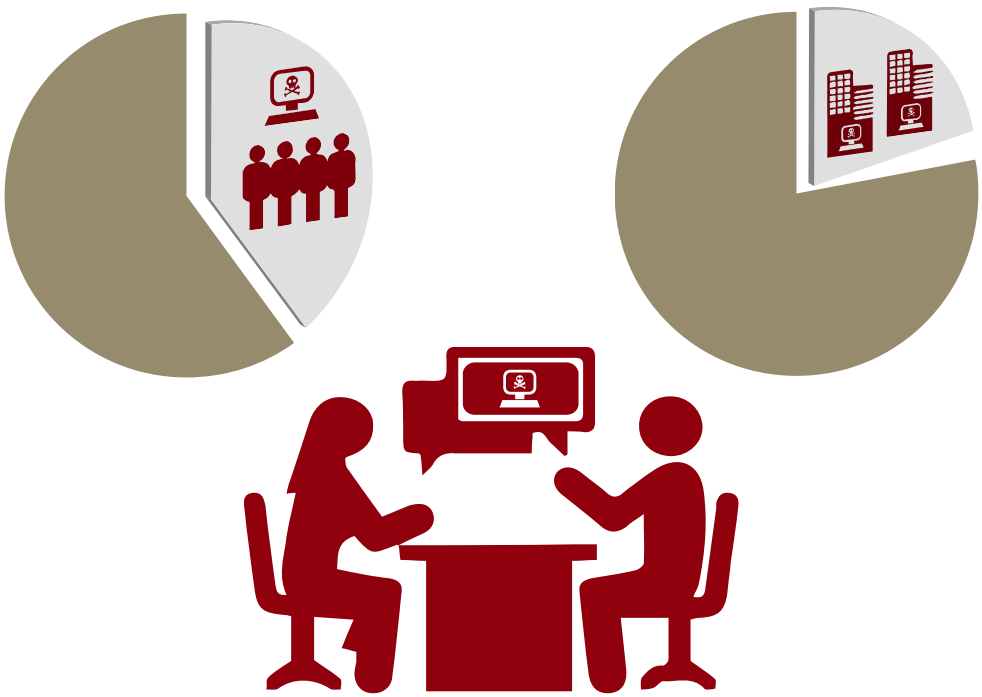
Cybercrime: The looming threat

Cybercrime rates in Thailand are increasingly rapidly. Twenty-two percent of our respondents stated that they were affected by cyber-attacks in the recent past. The results of the survey show that the incidence of reported cybercrime among our respondents increased sharply in 2014 and 2015, jumping from fourth to second highest compared to the result in year 2012 and 2013.

We believe that as more organisations venture into the Internet of Things in Thailand, the risk from cybercrime will multiply. PwC takes a closer look at our respondent's answers and insights into how Thai companies deal with cybercrime in Thailand.

Four in ten were aware of cybercrime.

But two in ten were attacked by cyber criminals.



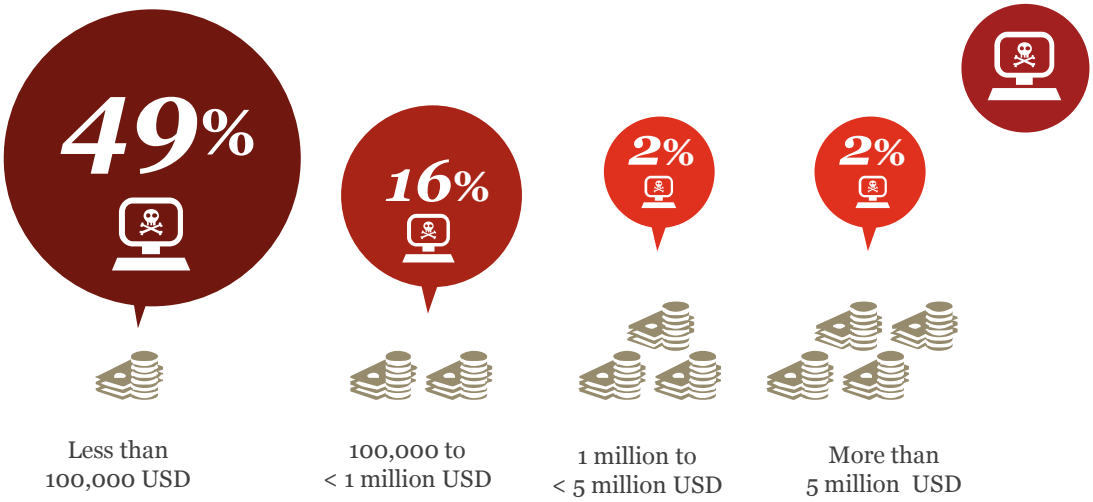
Who's affected?

Our survey found that all industries are at risk, particularly the financial services sector. According to PwC's 2016 Global State of Information Security Survey, the retail sector saw the most significant increase in cybercrime in 2015.

Internal and external threats

Unlike more traditional Thai industries that witness the majority of fraud being perpetrated by internal actors, 34% of the respondents said that the attackers were both internal and external, which is in line with global trends. While 44% reported that they were attacked by external actors. In our investigations in Thailand, attackers used the internet as the main channel to commit fraud. We recommend developing robust IT policies and systems that are in line with global practices to meet the threat of internal and external cyber-attack, even within your corporate IT department.

Financial damage caused by cybercrime in 2014 and 2015



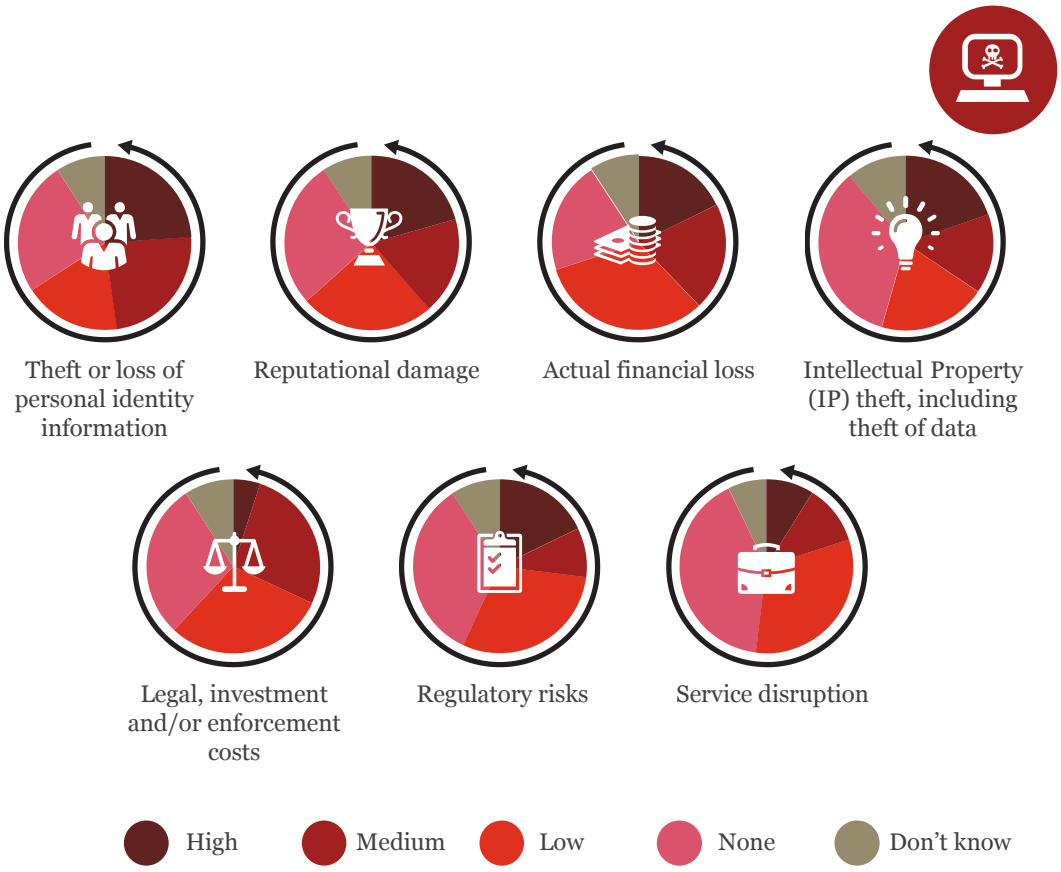
Losses sustained from cybercrime

One-fifth of victims in Thailand reported losses of more than $100,000 (approximately 3.5 million baht). Another 4% reported losses through cybercrime of $1 million and above (approximately 35 million baht and above). A point to be noted is that 16% of respondents indicated that they had suffered losses between $100,000 and $1 million to cybercrime attacks. Unlike traditional forms of economic fraud, cybercrime can target a number of industries, exposing weaknesses and causing financial damage of larger proportions and increased frequency.

Loss of personal identify information the most damaging

Among survey respondents, theft of personal identity information was considered the most damaging outcome of a cybercrime, followed closely by reputational damage and intellectual property loss. Stealing of intellectual property and trade secrets are common based on our past investigative experience.

Non-financial damage caused from cybercrime in 2014 and 2015

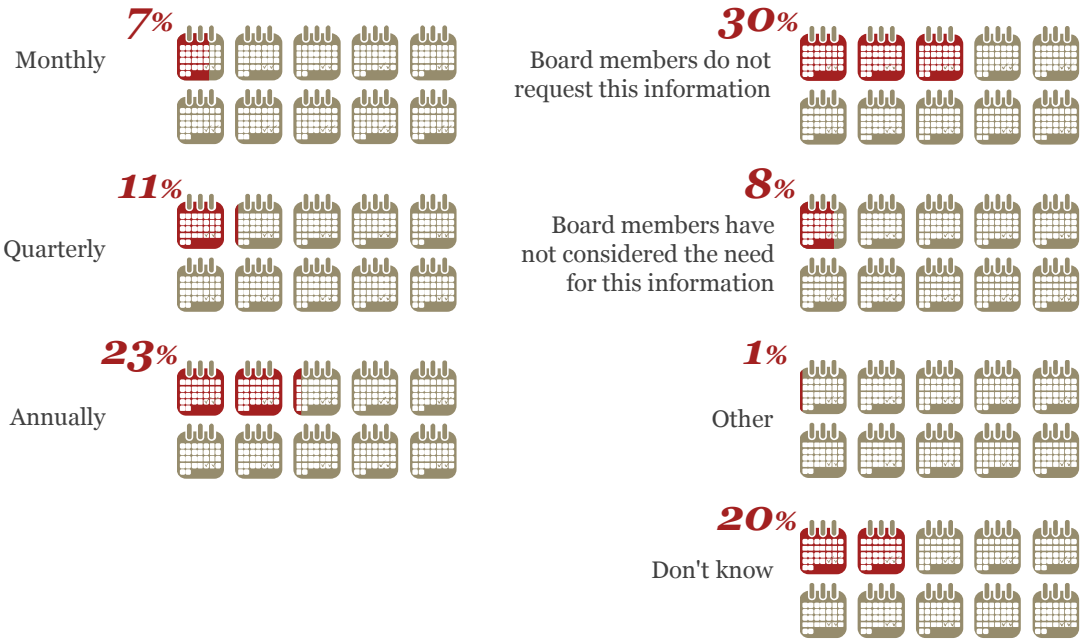


What Thai companies are doing about cybercrime

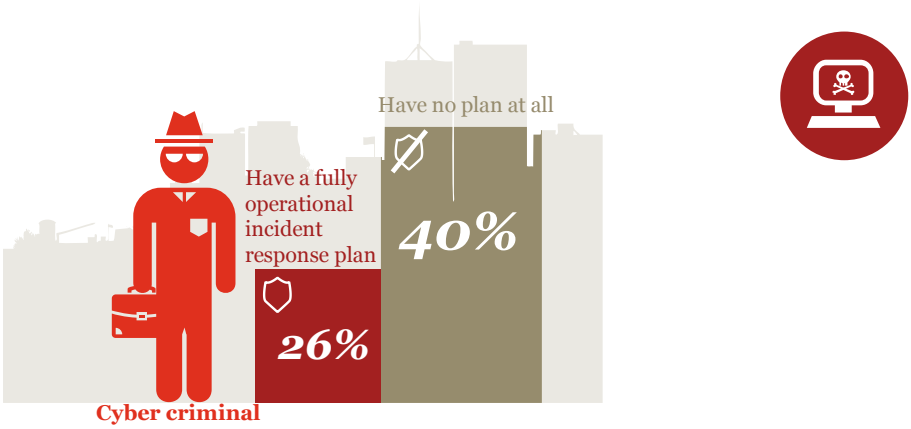
Organisations globally have begun to respond more rapidly, investigate, and remediate cyber incidents using proactive cyber threat assessments through forensic techniques. While 39% of the respondents believed their awareness of cybercrime fraud increased over the previous year, Thailand, unfortunately, has not caught up with the global trend and is still dealing with fraud incidents after the fact.

In Thailand, only 41% of board members requested information about their organisation's state of readiness to deal with cybercrime. Only 26% of Thai organisations have fully-operational incident response plans, compared to the global average of 37%. Four-in-ten have no plan at all, and of these, nearly half don't think they need one, which is alarming considering Thailand is at the forefront of cyberattacks.

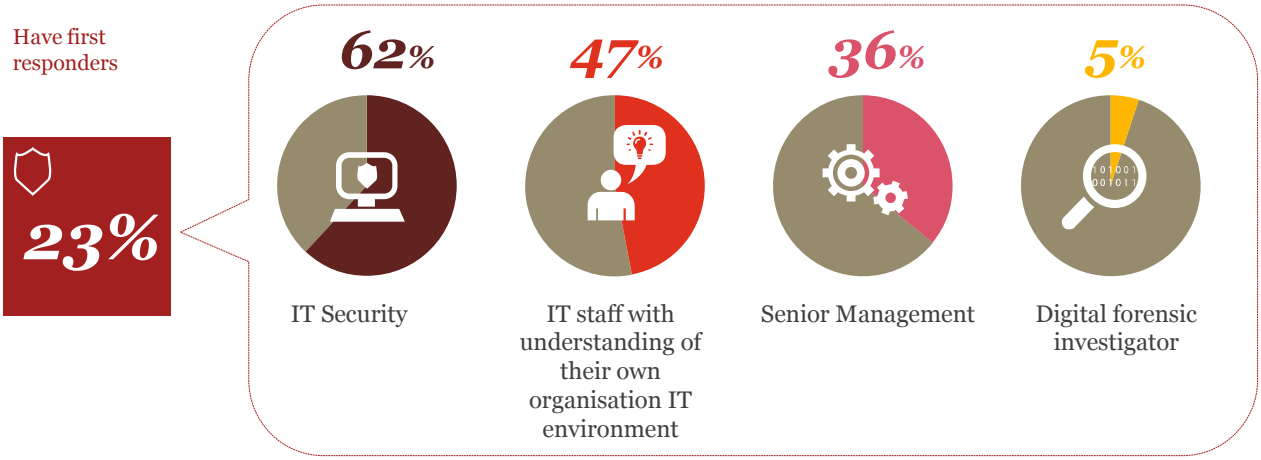
How often do board members request information about their organisation's state of readiness to deal with cybercrime?



Globally, 37% of respondents – most of them in the heavily-regulated financial services industry – have a fully operational incident response plan, while in Thailand the average is just 26%.

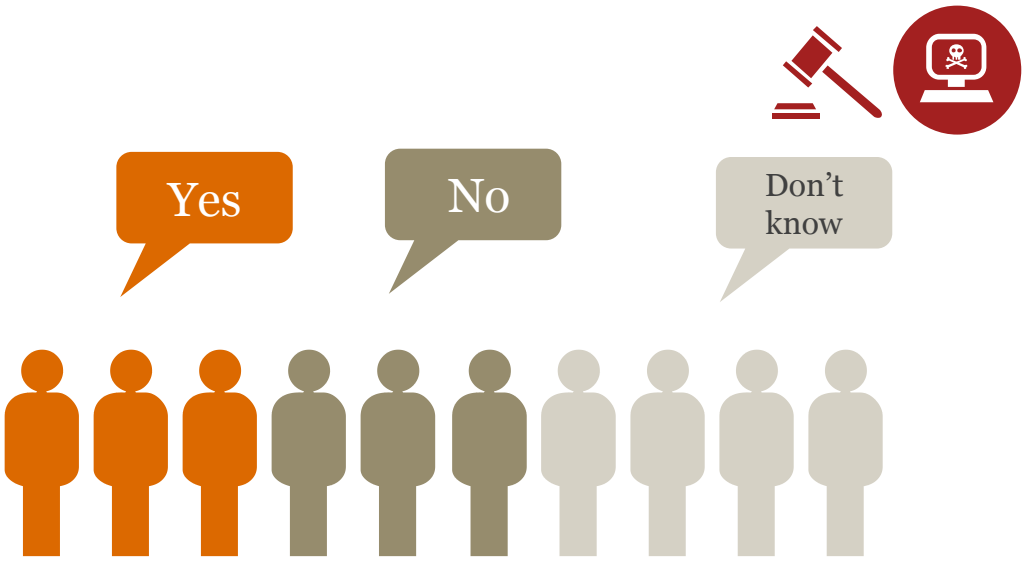


Eighty percent of the respondents stated that they do not have teams in place to act as the first respondent to cyberattacks. And, of the 20% who stated that they do have a cyber attack incident team, only 5% stated that these teams include digital forensic investigators.



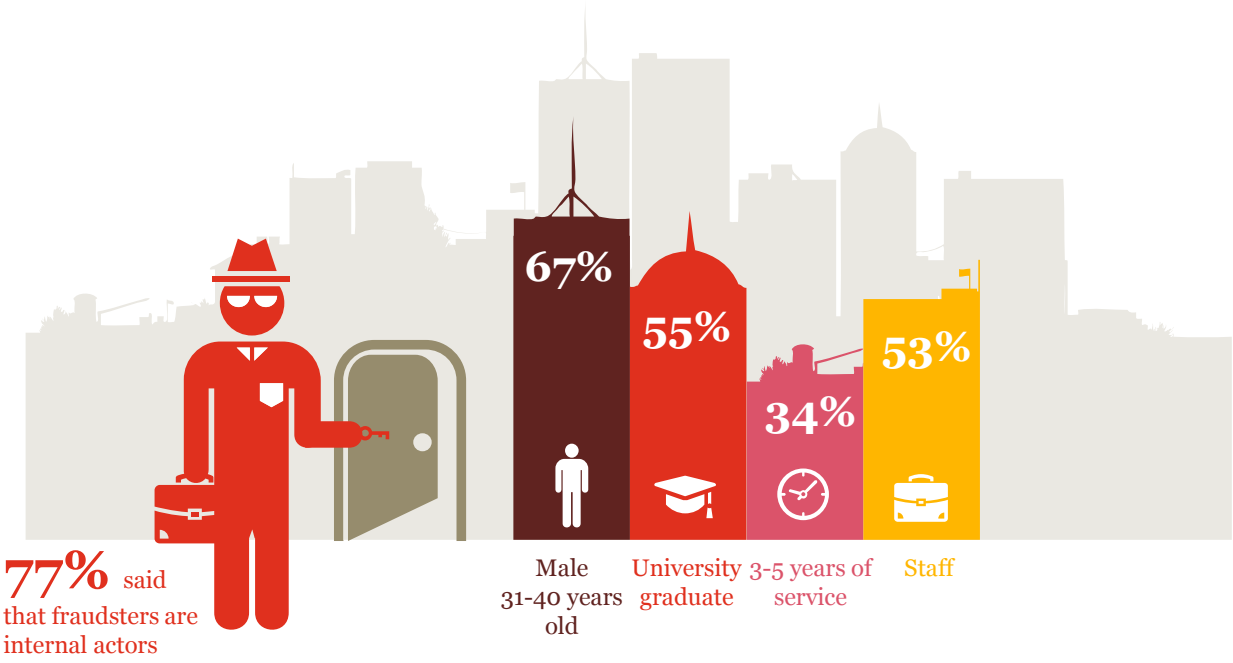
These numbers, coupled with the fact that 70% of respondents do not believe or were not aware that Thailand law enforcement agencies have the skills and resources to investigate cybercrime, present an inadequate systems that cannot prevent cybercrime and ultimately may fail to prosecute the perpetrator.

Confidence in law enforcement agencies



More than half of respondents said that their staff commit fraud.

Who are the fraudsters?



Fraudster's profile in Thailand

In Thailand, employees continue to be the dominant actors in fraud cases, although the rate dropped to 77% from 89% in 2014. Interestingly, the fraud profile in Thailand has moved from middle management (56% in 2014) to staff who now make up more than half, which is an increase from 36% in 2014. This could be due to increases in their authority and responsibilities.

Three-in-ten (31%) victims said that the external fraudsters are business partners or agents acting on behalf of the companies. One-third (33%) of companies operating in Thailand said that they reported the crime to law enforcement, which is significantly lower than the global statistic (53%). From these incidents, only 17% ended their business relationship, compared to the South East Asia rate of 27%.

To mitigate this risk, organisations need to conduct proper due diligence on business partners, agents, intermediaries, and other counterparties that are acting on behalf of their companies.

Fraud motivation

In line with the global trend, most respondents in Thailand believe that opportunity and ability to commit fraud is the biggest motivator to do so. Employee morale can also play a role in fraud risk: disgruntled staff are more likely to cheat their employers. This highlights the need for effective internal controls for fraud prevention and detection, such as a whistleblowing programme.

Response to fraud and allegations

Fraud allegations must be taken seriously and companies should seek professional advice for handling fraud allegations. Although the legal process can be time consuming, taking legal action carries a higher chance of future deterrence.

Sixty-eight percent of Thai organisations dismissed employees for participating in fraud compared to the global average of 76%. Five in ten informed law enforcement, while four in ten took civil action. Only 14% informed regulatory authorities, lower than the South East Asia average of 22%.

Types of punitive action taken against internal perpetrators

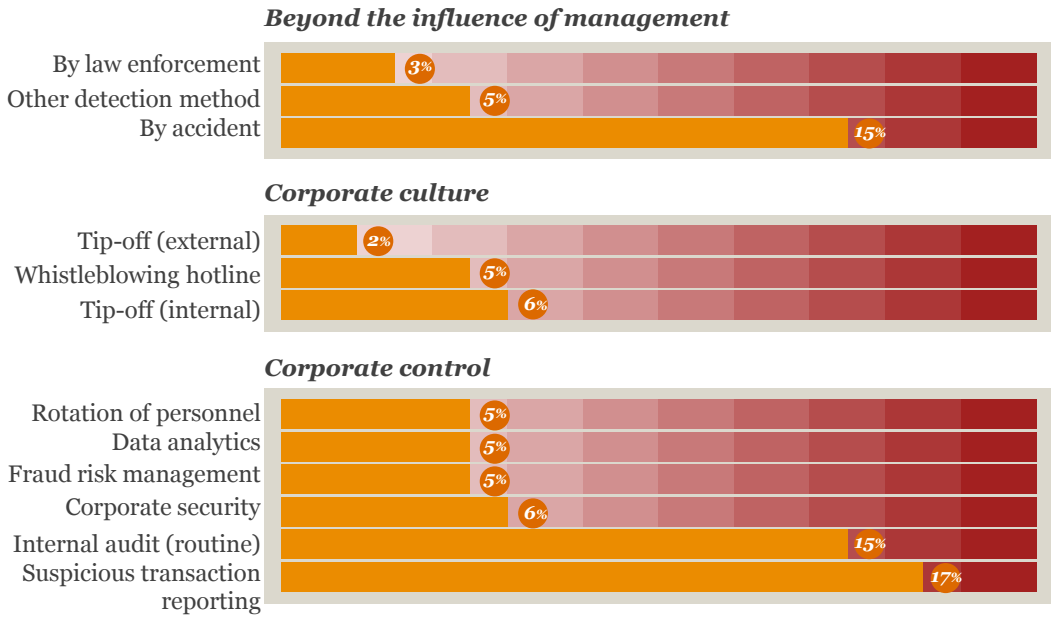
Thai organisations remain below global standards for fraud risk management and have a higher tolerance for red flags.

Fraud detection methods

This survey shows that fraud is often detected by the reporting of suspicious transactions (17%), followed by routine internal audits. Fifteen percent of the survey respondents stated that incidents of fraud were discovered by accident. Only 13% of Thai organisations said that fraud was detected by internal and external tips, compared with 23% regionally and 17% globally.

Compared to the global trends, a limited number of fraud cases in Thailand were detected via tip-off and whistleblowing hotlines, which suggests that companies in Thailand are yet to implement robust internal practices and strengthen the corporate culture of speaking up to detect fraud effectively.

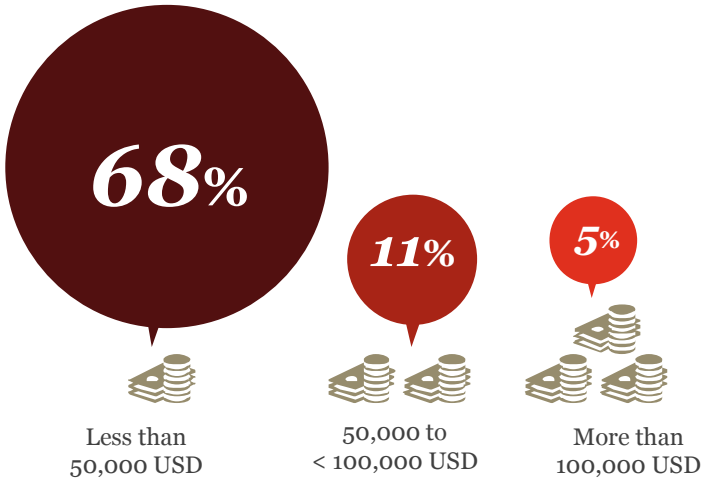
How economic crime was initially detected



Based on our experience, a robust and effective Whistleblowing Programme Framework provides communication channels to receive information on suspicious activities or unethical/illegal practices and detect misconduct. We suggested that companies review whether existing *whistleblowing policies* comply with existing standards and promote hotline awareness to encourage employees to report anything suspicious. We also encourage workshops for hotline operators and conducting interview training.

Nearly 70% of respondents said that during the past two years, their company had spent less than $50,000 or 1.75 million baht to investigate economic crime while about 10% spent between $50,000 and $100,000 (between 1.75 million and 3.5 million baht). Another 5% said that their budget is $100,000 and above (approximately 3.5 million baht and above).

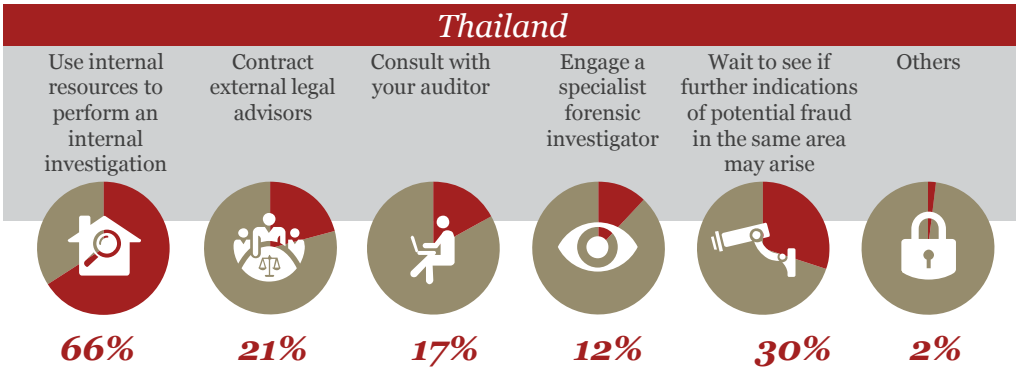
Budget spent on investigations and/or other interventions as a result of economic crime in 2014 and 2015



Nearly half of Thai companies perform a proactive fraud risk assessment at least once a year, while about one-quarter said that they have done none at all. Only 15% of respondents mentioned that their organisation has performed an assessment more than once per year, compared to the global average at 20%.

A worrying **26%** of organisations have not carried out a fraud risk assessment in the past 2 years.

What action would you take after discovering fraud?



Which actions are likely to be taken?

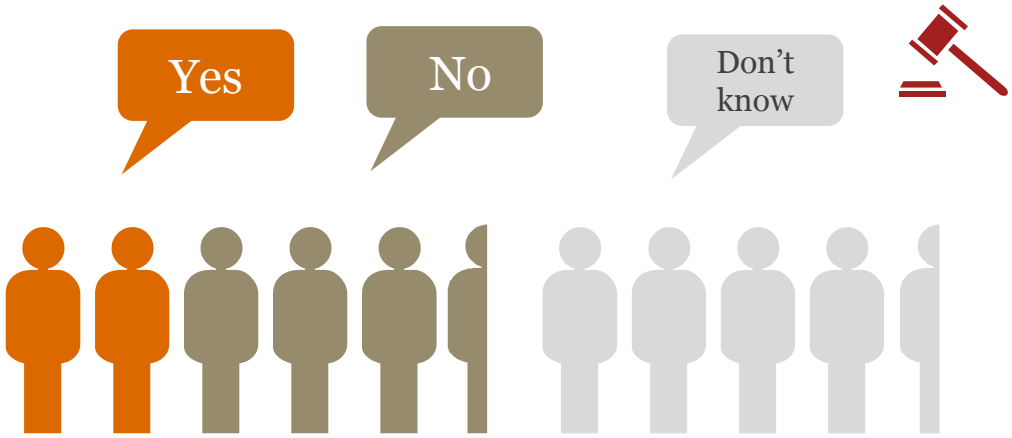
Thai organisations remain below global standards in terms of fraud risk management. When potential fraud was detected, Thai companies (66%) tend to use their internal resources to investigate, rather than seek external expert advice.

Respondents in Thailand are less likely to contact external legal advisors (21%); while 17% consulted their auditors and only 12% engaged a specialist forensic investigator. More alarmingly, three-in-ten companies did nothing and waited for further indicators of potential fraud in the same areas.

Strength of law enforcement in fighting economic crime

Asking whether Thai law enforcement agencies are adequately resourced and trained to investigate and prosecute economic crime, 33% responded in the negative and a further 44% said they don't know. In other words, fewer Thai organisations (23%) have confidence in law enforcement agencies, compared to the global average of 28%.

Confidence in law enforcement agencies



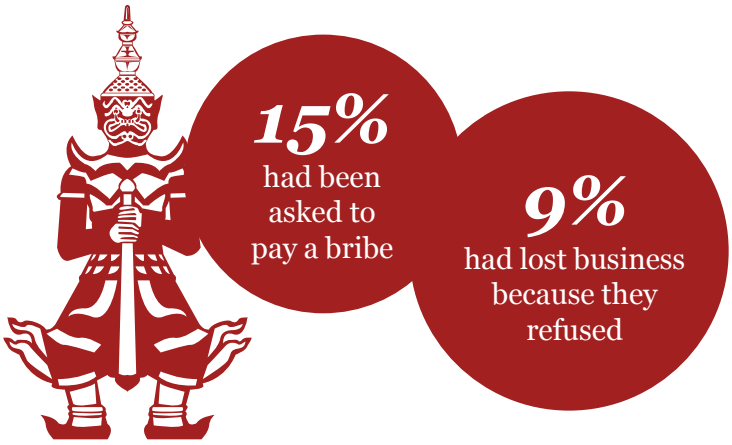
Fifteen percent of organisations has been asked to pay a bribe while 21% say they did not know.

Ethics & Compliance

Nearly one in ten (9%) believed that in the past two years, they have lost an opportunity to a competitor that paid a bribe. Almost nine in ten respondents (85%) believed that their top management makes it clear that bribery is not a legitimate practice, while 84% believe that their top management takes a public stand against corruption and 75% expected that the government would actively fight corruption in the coming years.

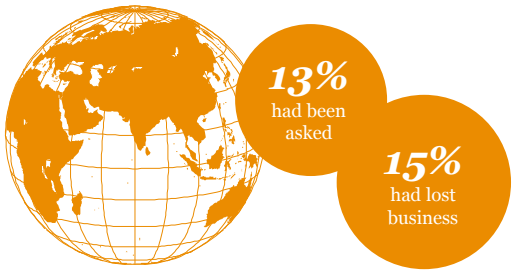
However, one in four respondents (25%) expect to experience bribery and corruption in the next two years.

In the last two years



Thailand

Asia Pacific



Global

Is your compliance framework working effectively?

Our survey revealed that a significant number of businesses have no formal compliance structures. In some cases, this may be due to the small size of the companies. Approximately one-in-five (20%) companies in Thailand have no formal ethics and compliance programmes in place, compared to 18% globally.

Who is in charge of the compliance programme?

46% said that the CCO is responsible for the business ethics and compliance programme.

How do you monitor your compliance programmes?

70% rely on their internal audit to ensure the effectiveness of compliance programmes.

Of the 80% of organisations who do have a formal business ethics and compliance programme, responsibility for the programmes is widely dispersed among individuals at the company. This can make reporting and remediation unclear and ultimately weaken the anti-fraud structures within an organisation.

In Thailand, roughly half of respondents (46%) reported that their organisation's chief compliance officer (CCO) was responsible for their business ethics and compliance programme. In smaller organisations — some of which may not have a CCO, and where compliance responsibility is more likely to sit with HR, the CAE or the CFO — this number was, unsurprisingly, lower still (31%).

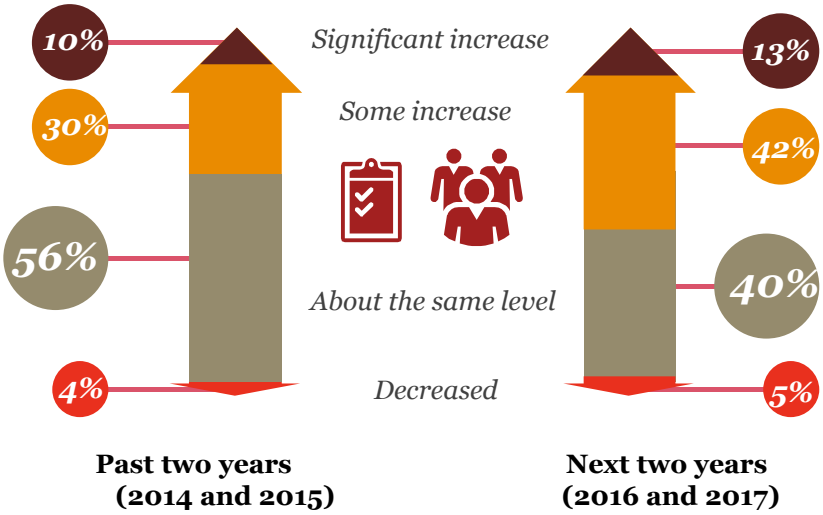
As mentioned earlier, about six in ten (64%) believe that opportunity is the main driver of internal fraud – far outweighing the other two elements of the fraud triangle: incentive/pressure and rationalisation. About 70% of respondents reported that they are relying on their internal audits (IA) as part of their approach to assess the effectiveness of their compliance programmes.

Are internal audits enough?

Our experience shows that internal audits — while important for assessing compliance effectiveness — are not sufficient for assuring compliance, because they are both periodic and historical. Also, audits rely primarily on disclosure and almost never involve investigating large sampling of transactions or verifying the authenticity of submitted documents.

Since prevention must occur at the point of decision making, not after, IA should be combined with management reporting and real-time transaction monitoring so that issues are promptly detected and prevented in time. Our financial-sector respondents in particular point to management reporting as a key tool for ensuring the effectiveness of compliance programmes — as did COOs and CSOs (65% and 63%, versus an average of 54%). Currently only 8% of respondents say they are using other internal monitoring approaches such as the data analytics application to identify high-risk transactions.

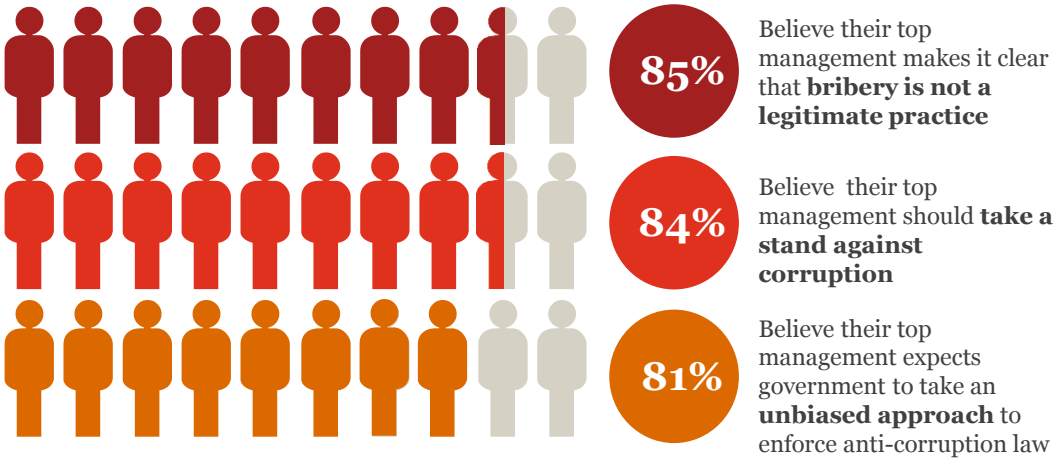
How is your organisation responding to the threat of economic crime in terms of its compliance programme and resource spend?



Our survey also asked about the compliance programmes and internal resources spent to combat economic crime. Overall, 55% of Thailand-based companies will strengthen their compliance programmes and resources to combat economic crime.

Our respondents reported that the greatest damage from economic crime was not the impact to the share prices or relationships with regulators, but to employee morale. Damage to employee morale received a 50% rating for medium to high impact, with reputation damage receiving 47%. In both cases, the nature of how a business is *perceived* — from the inside as well as the outside — was the greatest concern. This underscores the key role that ethics and values play in a successful business strategy.

Almost nine in ten respondents (85%) believe that their top management makes it clear that bribery is not a legitimate practice, 84% believe their top management should take a public stand against corruption and 81% believe the government should be unbiased in enforcing anti-corruption law. But, 25% still expect to experience bribery and corruption.



More than half of financial services still rely heavily on human reporting methods to identify suspicious activity.

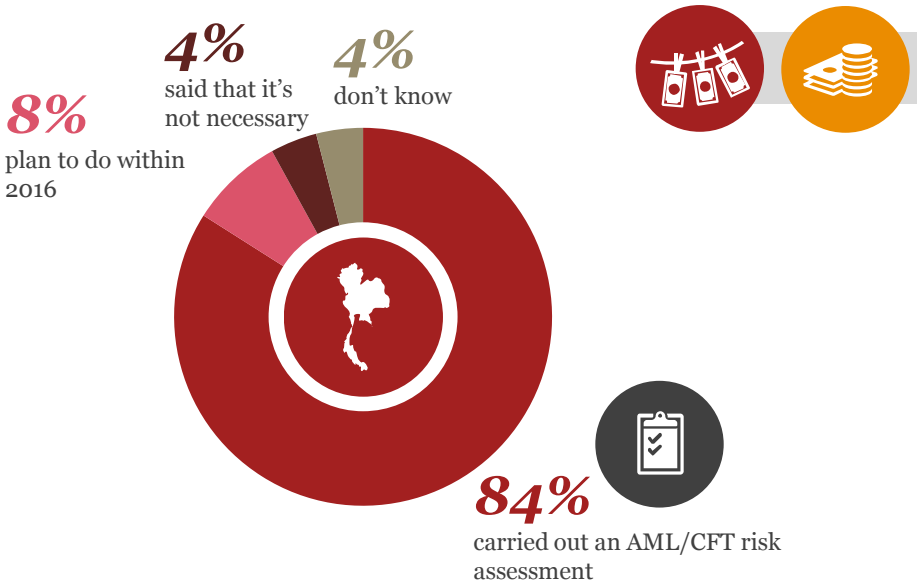
Anti-Money Laundering

Government reforms

The Thai government has instituted a number of reforms to boost anti-money laundering and counter terrorism financing measures. These developments come in response to both local pressure such as from Thailand's Anti-Money Laundering Office, and international obligations such as of anti-money laundering requirements Asia/Pacific Group on Money Laundering, of which Thailand has been a member since 2001.

The government has improved AML rules under an initiative that started in the third quarter of 2015. Improvements include Revenue Department legislation to strengthen tax enforcement, tighter measures for cross-border movement of bearer instruments, and closer coordination with the Ministry of Foreign Affairs to enforce counter terrorism financing measures. The National Council for Peace and Order (NCPO), the current military government, also announced a broader anti-corruption crackdown in February 2016 that could affect AML measures.

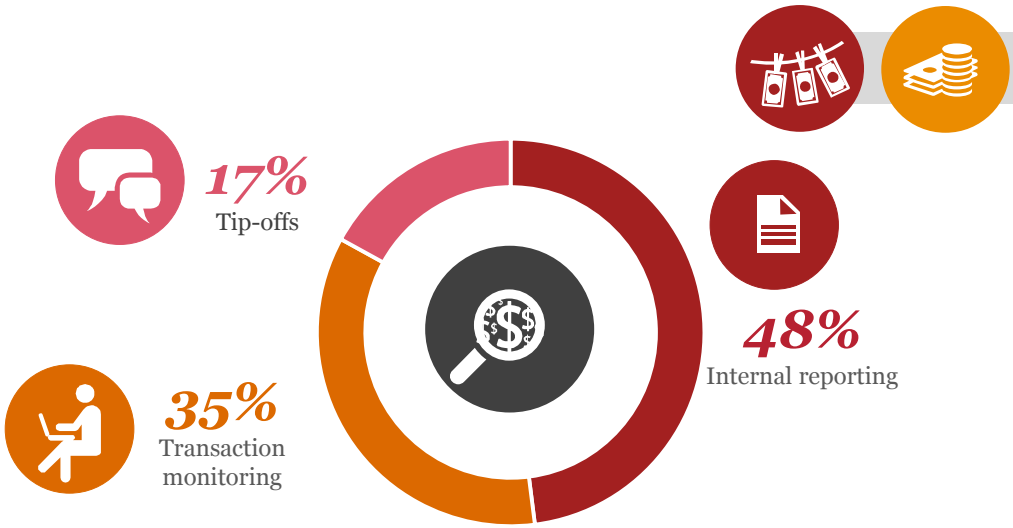
AML/CFT risk assessment performed by financial services operating in Thailand



Enforcing AML rules in Thailand carries special challenges. The economy is largely cash based, making it difficult to track and monitor payments both locally and internationally. Corruption and politicisation also create challenges and give well-connected figures opportunities to circumvent controls and evade enforcement.

Despite the challenges, Thailand's AML enforcement has improved. In addition to local measures under the Economic Crimes Suppression Division of the Royal Thai Police, the country is subject to spot inspections by the Financial Action Task Force on Money Laundering, whose findings impact Thailand's international standing both politically and economically. Our survey results reflect this tighter enforcement, and 84% of respondents stated their organisation has done anti-money laundering and counter terrorism financing (AML/CTF) risk assessments.

Methods used by financial services to identify suspicious money laundering/financing of terrorism activity



There is increasing attention on Thailand's AML performance, and our survey provides insights into the methods that Thai organisations use to detect money laundering issues. It shows that most of the respondents rely on internal reporting, indicating that organisations still rely heavily on human reporting methods.

Meanwhile, many are using automated transaction monitoring methods (35%), which enable financial institutions to assess customers' transaction behaviour systematically. These analyse trends in underlying customer transactions and generate automated alerts for indications of potential money laundering activities and fraudulent transactions.

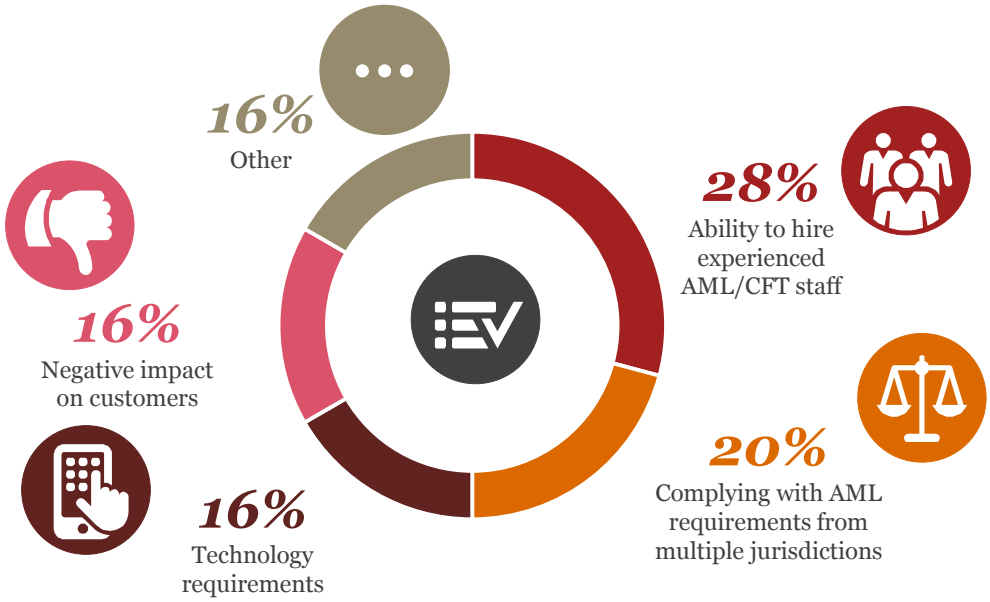
From our experience, we recommend companies use technology to automate fraud detection that continuously monitor transactions. Therefore, management can respond quickly to red flags and reduce the risk of fraud escalation.

Challenges that companies face

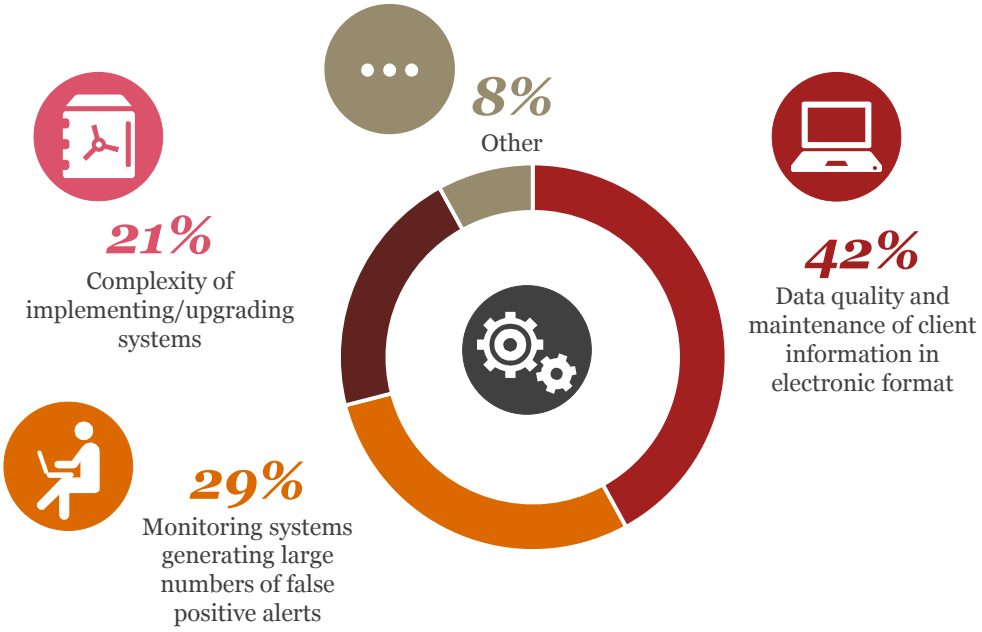
The biggest challenge in relation to complying with your local AML/CFT requirements is the ability to hire experienced AML/CFT staff. Twenty-percent also mentioned complying with AML requirements from multiple jurisdictions, then technology requirements and the negative impact on customers (each at 16%) as challenges associated with AML/CFT.

The majority of financial institutions (42%) say the biggest challenge to their AML systems is data quality, followed by issues with monitoring systems (29%), and complexity of implementing and upgrading systems (21%).

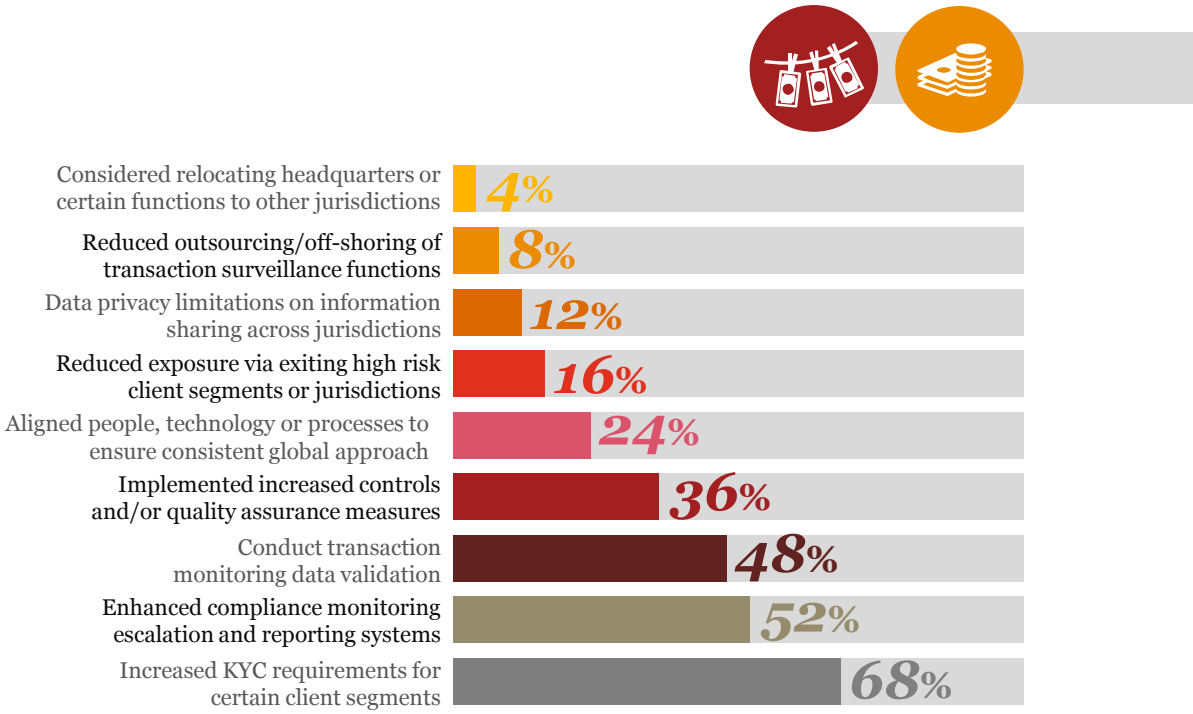
Top 3 challenges in relation to complying with local AML/CFT requirements



Top 3 challenges in relation to complying with local AML/CFT systems



Activities implemented by financial services to reduce AML/CFT risks



To reduce AML/CFT risks, 68% of financial services companies in Thailand increased 'know your customer' (KYC) requirements for certain client segments, while half enhanced compliance monitoring escalation and reporting systems.

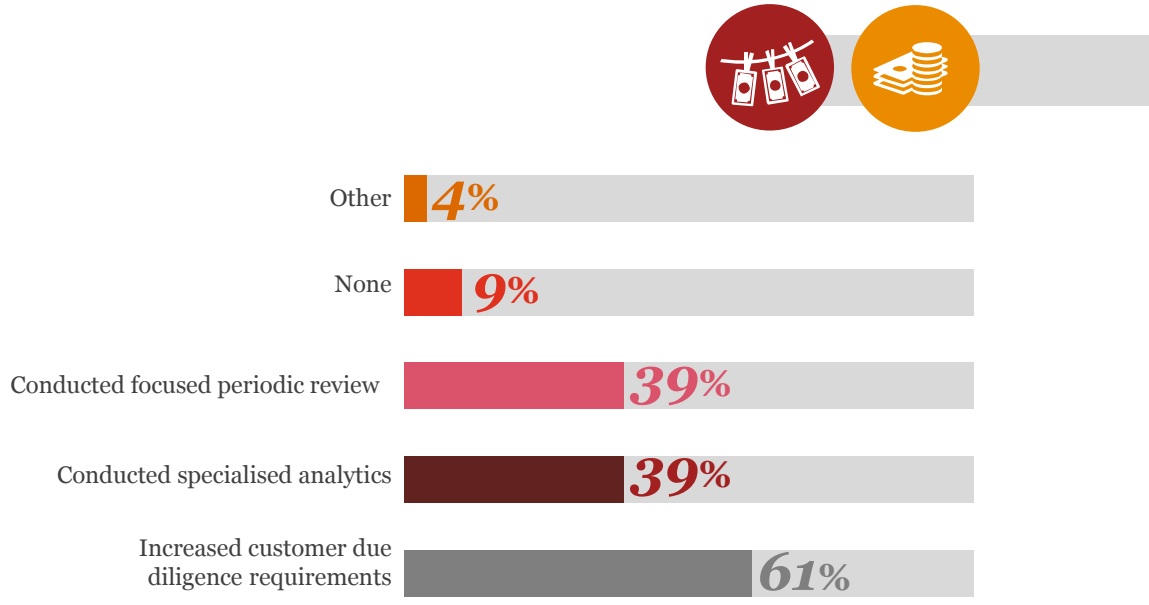
Fewer companies aligned people, technology or processes with the global approaches (24%). This is actually an important part of compliance, and we recommend that companies perform gap analyses to identify and rectify gaps to ensure that their processes and systems are consistent across the enterprise.

While stricter AML measures do not generate revenue, they often translate to much lower risks for both legal issues and reputational damage. One benefit of successful compliance programmes is reducing unsecured exposures from high-risk clients. This can help the company manage and control risk appropriately. Reducing loan-loss provisions is included.

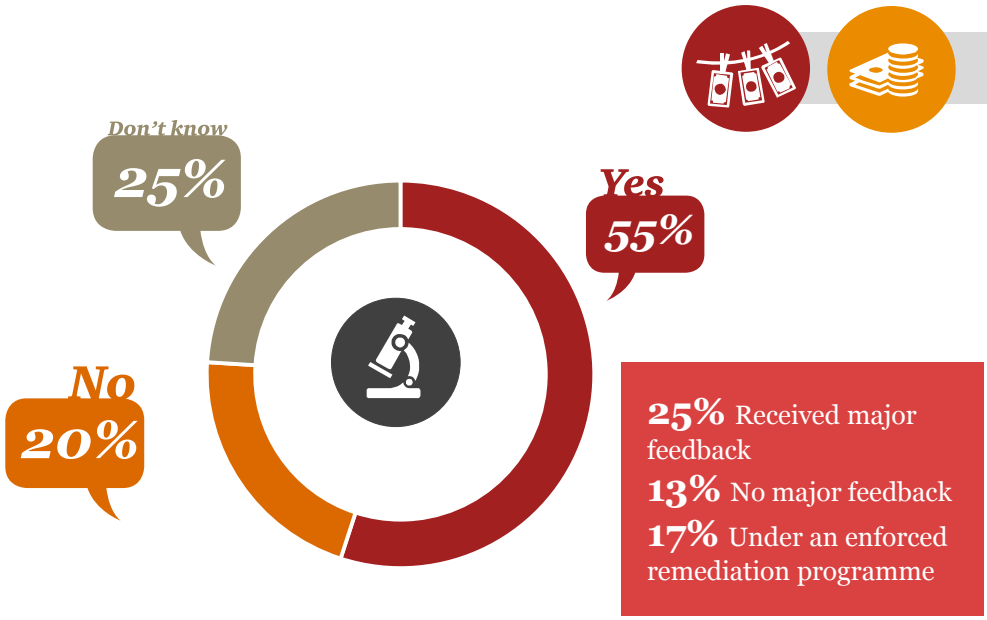
Most Thai financial services companies detect and deter money laundering by increasing their customer due diligence requirements in the industries targeted by regulators for increased scrutiny. Only four in ten used specialised analytics to identify unusual trade practices/patterns consistent with under or over-payment of goods/services; and conducted focused periodic reviews of holistic activity for clients involved in high risk businesses or jurisdictions. One in ten took no measures. This indicates that some companies are not aware of this risk.

Due diligence measures are an important part of risk management and should include scrutinising related-party relationships and identifying ultimate beneficial owners. These measures are especially important if the company is working in the high-risk areas such as in bordering provinces, where illegal funds can flow across international borders. Specialised analytics helps with this by identifying unusual trade practices and patterns, such as under or over-payment of goods and services.

Measures implemented by financial services to detect and deter trade based money laundering activity



Regulatory enforcement/inspection in relation to AML experienced by financial services in 2014 and 2015



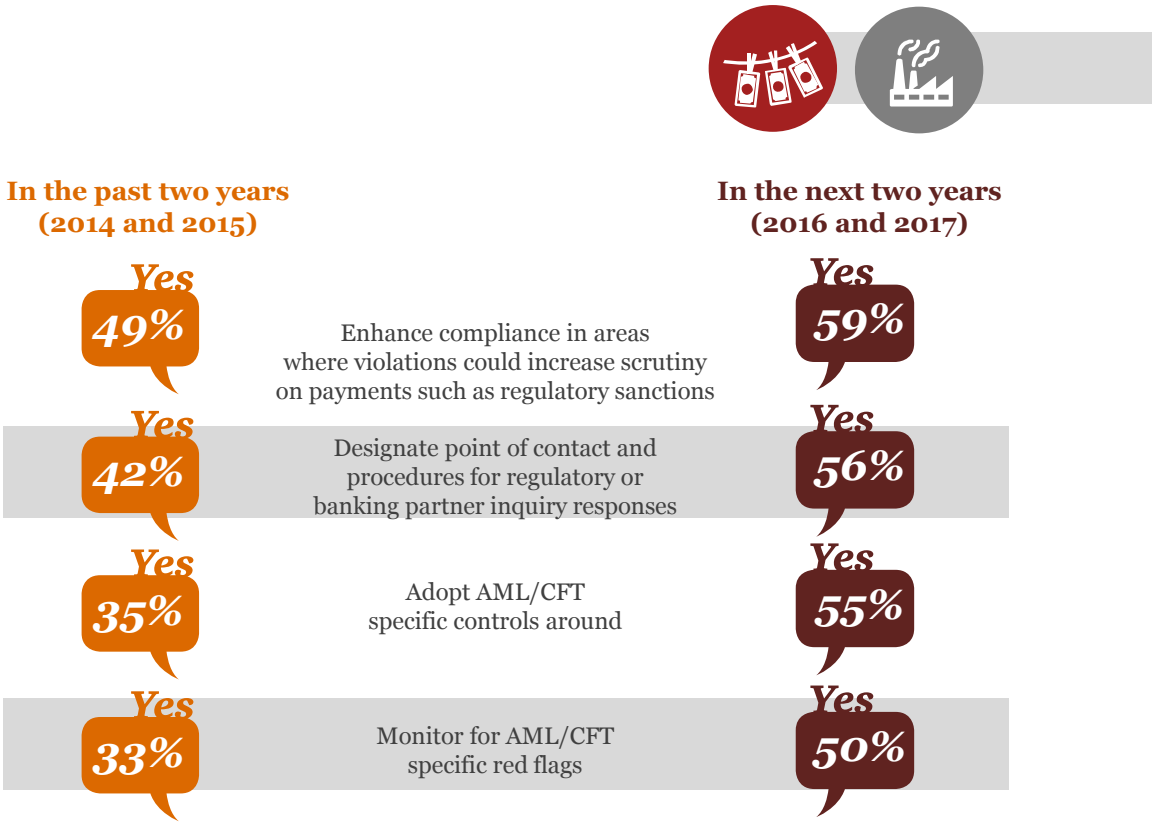
A full quarter of financial services respondents had been subjected to a regulatory inspection that resulted in major issues to address. Another 17% were under enforced remediation programmes.

Measures implemented by financial services to address increased regulatory expectations

Nearly half of the respondents said that their companies are conducting training focused on an aligned approach to compliance. In addition, 36% had hired additional compliance resources into roles for specific regulations such as AML/CFT, Anti-Bribery & Corruption, and Sanctions.

To detect and deter trade-based ML, 32% of financial services restructured departments responsible for governance and compliance. Meanwhile, almost three in ten financial institutions increased internal communication or collaboration, and expanded the role of exiting governance and compliance staff to cover additional areas of the organisation.

Measures implemented/planning to implement by non-financial services companies based in Thailand



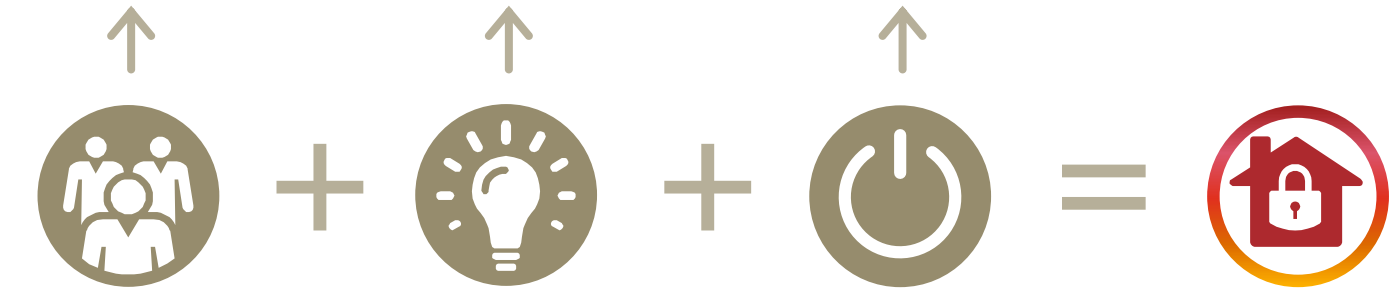
More companies in the non-financial sector will put more effort into anti-money laundering activities. Fifty-five percent of respondents said that their companies will adopt AML/CFT specific controls, around a 20% increase between 2014-2015 and 2016-2017. Additionally, half of non-financial organisations will monitor for AML/CFT specific red flags, from 33% in 2014-2015 to 50% in 2016-2017.

Measures taken by non-financial services companies to limit exposure to trade-based money laundering activity

Of the non-financial institutions in Thailand, 34% admitted they have taken no measures to reduce trade-based money laundering risks. Almost half of respondents said that their organisation has established internal controls around payments to/from third parties to limit exposure to trade-based money laundering activity. About one-third of non-financial institutions specifically prohibit unusually complex transactions and conducted third party due diligence at the beginning of the relationship.

Under the AML rule, not all non-financial businesses are required to report transactions that exceed the values prescribed in the relevant ministerial regulations. Only traders in jewellery, car dealers, and real estate brokers are subject to the enforcement under the Act. Although it's not a mandatory requirement by regulators, the non-financial industry should be aware that money laundering activity can impact their businesses by facilitating economic crime, which in turn suppresses their business growth.

1. *Develop clear anti-fraud and anti-bribery programmes*
2. *Appoint independent staff to monitor and implement the programmes*
3. *Communicate policies and measures throughout the organisation*
4. *Intelligent scoping to investigate and act on fraud cases*
5. *Don't downsize risk/compliance management team when risks are rising*
6. *Tailor anti-fraud policies and structures to Thailand's unique fraud risks*
7. *Formalise your incident response and remediation process*



Call to action

Seven steps to preventing and fighting fraud

Contact

Vorapong Sutanont
Partner
Tel: +66 (0) 2344 1000
Fax: +66 (0) 2286 4440
Email: vorapong.sutanont@th.pwc.com

www.pwc.com/th

© 2016 PricewaterhouseCoopers Consulting (Thailand) Ltd. All rights reserved. PwC refers to the Thailand member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.