Economic crime in Thailand

pwc

Contents

Foreword

For the second year in a row, PwC's Global Economic Crime Survey has polled decision makers in Thailand to understand the scope and depth of fraud in our country. And for the second year, we have seen an increase in fraud nearly across the board. Many of the key categories are significant when compared to international levels.

These results do compare with our experience at the Thailand Forensics practice, where clients have reported costly and damaging fraud ranging from high- to low-tech. The issues span across sectors and include the theft of materials from manufacturing sites, hacking and financial fraud at banks, and dummy companies being used to rig bids and skim profits from construction firms. These schemes not only cause direct financial damage, but also undermine product quality and expose victims to lawsuits and reputational harm. The survey shows that one-third of respondents experienced these types of crimes. We also expect this type of crime to grow.

However, even with the increasingly high value and sophistication of frauds in Thailand, we have worked hard to stay one step ahead. We've done this by constantly upgrading our technology and investigative training. We've also stayed informed about the latest anti-fraud developments of through our network in law enforcement and the specialist within the business community.

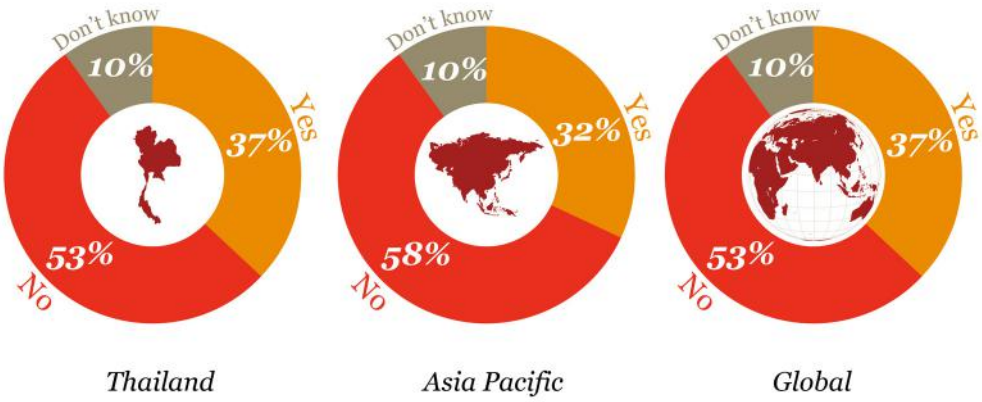
Thailand has always been a medium-to high-level fraud risk area and the political uncertainty in the past year have added to the challenges of doing business here. With greater awareness (facilitated by reports like this crime survey) organisations will be better equipped to capitalise on the many advantages offered by Thailand.

1. Economic Crime in Thailand

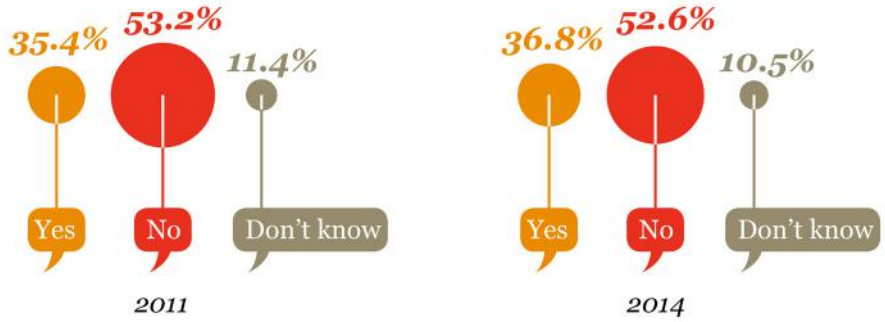
Our survey of local organisations found that economic crime is a growing threat to companies operating in Thailand. 37% of respondents indicated that they had directly experienced economic crime and 11% reported that they do not know if economic crime had taken place. Only 53% answered definitively that they have not experienced economic crime. This means that close to half are potential victims.

This ratio is not unique to Thailand and is in line with figures reported regionally and world-wide, suggesting that economic crime is not geographically or culturally defined.

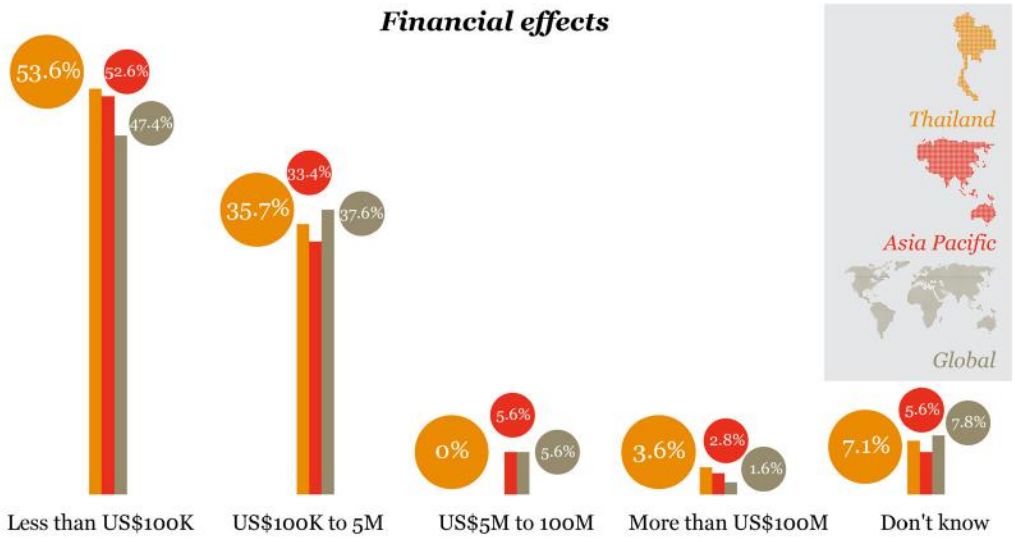
Has your organisation experienced economic crime?



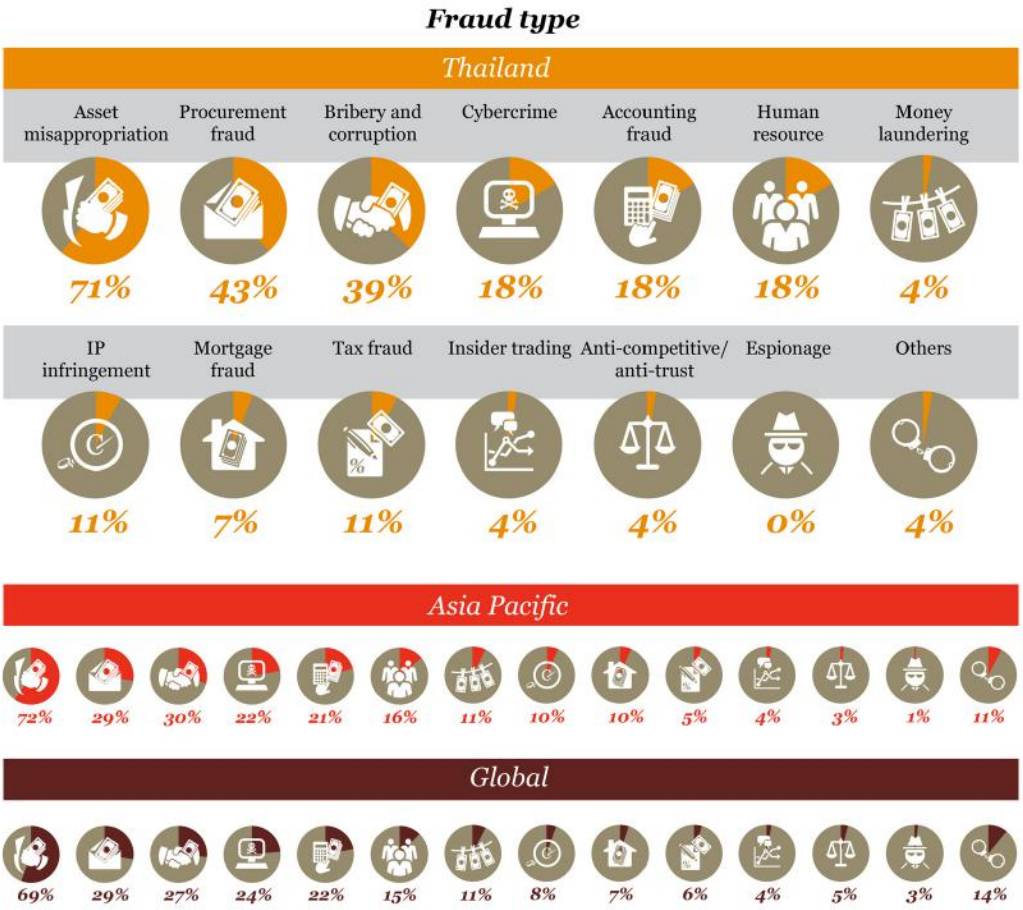
Has your organisation experienced economic crime? (Thailand)



Compared to three years ago, the percentage of companies in Thailand that have suffered economic crime is virtually unchanged. This could rise as awareness of economic crime increases and authorities enforce laws more rigorously.



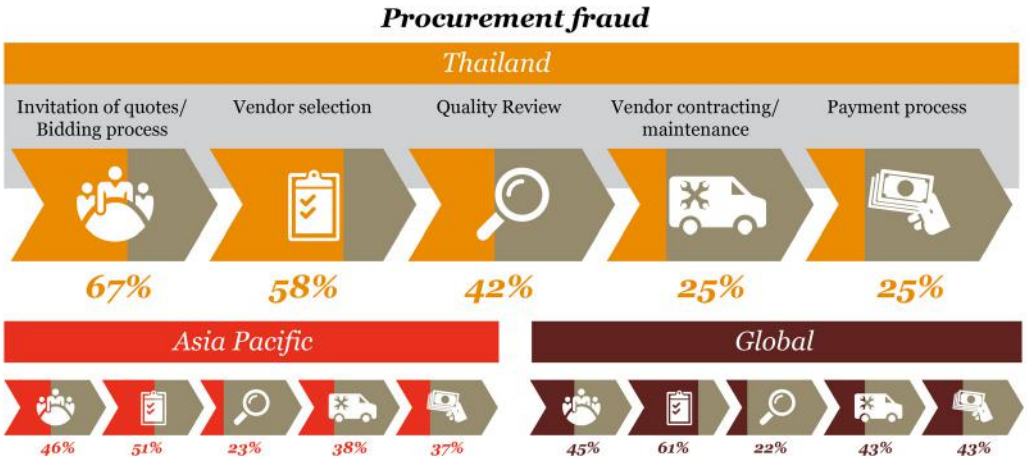
Economic crime is expected to remain a major problem for businesses and the most recent survey results demonstrate that the issue should not be treated lightly. While 15 fraud victim respondents in Thailand say they may have suffered damages of up to three million baht, 10 had suffered damages ranging from three to 150 million baht. The size of the damage varies according to the business size and the industry. While some respondents reported that the losses due to fraud may not have caused significant financial damage, they all said that fraud losses are unpredictable and therefore, they constitute an added business risk. Fraud damage is also difficult to calculate, and 5-7% of respondents were not certain of the size of the fraud damage to their organisation. This highlights the unpredictable nature of economic crime, and the need to put in place proactive programmes to reduce and deal with fraud.



Procurement fraud is a serious problem in Thailand and is the second-most common type of fraud encountered globally.

2. Procurement Fraud

Procurement fraud is a serious problem in Thailand and is also the second-most common type of fraud encountered globally. In Thailand, 43% of victims reported this type of fraud, compared to 29% globally. Procurement fraud normally occurs in the early stages of the transaction process and begins with the invitation of quotes and ends with payment. Looking at this breakdown, procurement fraud in Thailand is clearly most common at the beginning when potential vendors provide requested quotations. The threat appears to decrease throughout the process of vendor selection, quality review, vendor contracting and payment. This could be because of heightened internal controls and oversight in these internal processes. The findings in Thailand contrast with global responses, which show that fraud occurs fairly equally throughout the procurement process. The findings in Thailand suggest that organisations in Thailand would benefit greatly by strengthening their vendor selection criteria and tendering processes. Also, performing background checks and due diligence on perspective vendors is a good idea.



Survey respondents said that at the bid process stage, frauds were often committed through unverified vendors that had undeclared relationships with their employees. In some instances, vendors were discovered setting up shell companies to take part in bids and create the illusion of competition. This bid-rigging often involved cooperation from employees, who provided inside information or confidential pricing information that led to unfair competition.

Companies can stop this type of procurement fraud by strengthening screening procedures and asking themselves how they came to know individual vendors or vice-versa. A vendor could have approached the company during the normal course of business, or could have been introduced to the company via existing employees. That, in itself, is not always classed as fraud. But does the company know the relationship between its own employees and the vendor, and the risk this can cause? An engineer in the production department could 'lock' the specifications to favour a certain vendor. Also, a member of the purchasing department could reveal bids to vendors who may be relatives.

Our survey found that fraud often happens during the vendor-selection process because of lack of transparency, poor record keeping, and inability of management to thoroughly oversee such procedures. Companies also lacked vendor-selection criteria and gave too much autonomy for vendor selection to individual managers. There were often instances of risk caused by employee-vendor collusion that led to commercial kickbacks which in addition, happened regularly with the end user who involves with quality review of the products and services. Some of the main determinants of fraud were the strength of an organisation's guidelines for procurement and the rules around accepting vendor-paid customary 'new year' gift or sponsoring of 'staff party'. The right types of controls may vary for each unit within an organisation or between organisations. Companies must also conduct self-assessments or hire outside experts to conduct external forensic reviews. Too many controls will reduce flexibility and increase costs, but too few controls put the company at risk.

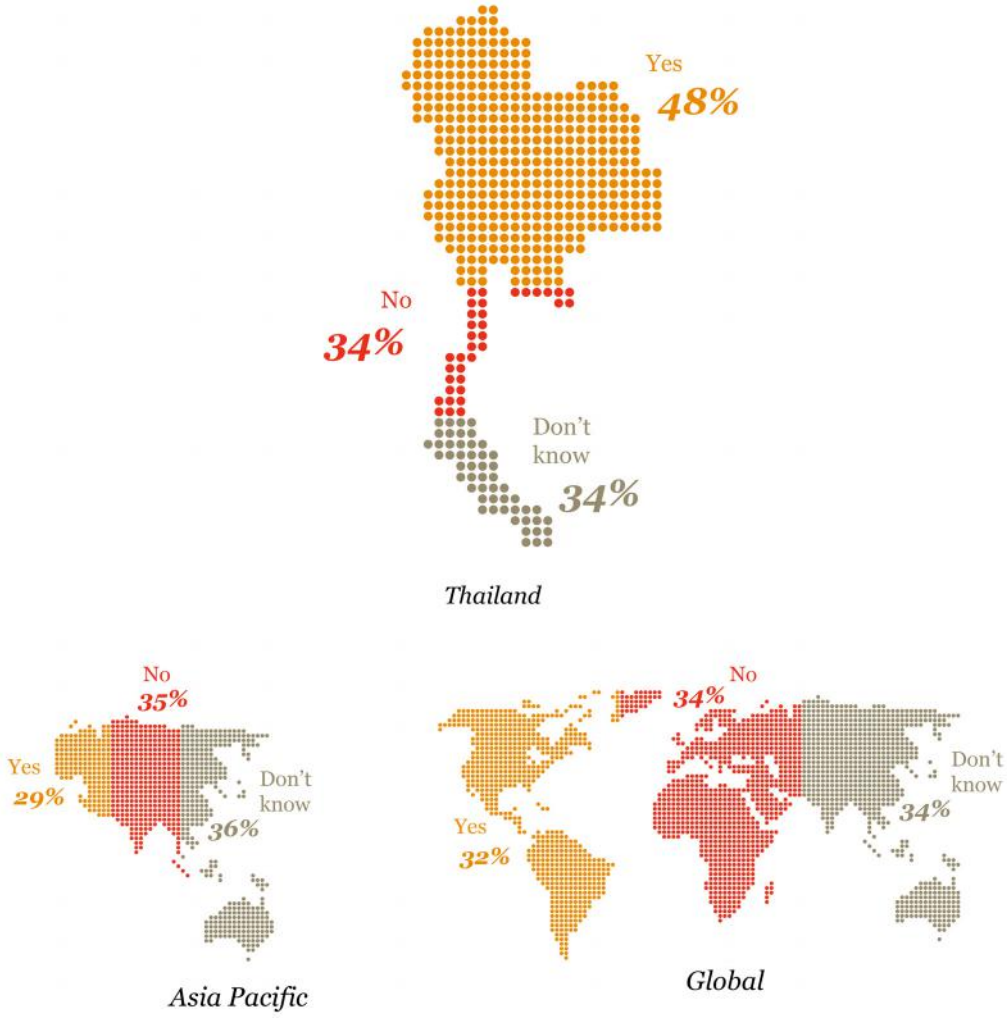
Procurement fraud is ultimately about the company overpaying for goods. Regardless of how a vendor wins the business, the company still has the opportunity to review or reject a vendor based on the quality of work or goods received. For example, did the vendors deliver the correct amount, or the correct specifications of goods that were agreed upon? In a typical business environment, procurement can be a process that spans many months and can involve many different people. Therefore, the staff members who receive the goods should be well trained to assess them, and there should be an effective control process to ensure a thorough review.

Likewise, procurement fraud at the payment process stage can come from weak internal controls. For example, a company should check that their employees have adequate documentation. They should also check if they have more of a 'family' attitude, where a trusting relationship can mean incomplete paperwork is accepted. Of course, in Thailand, most procurement fraud may have already occurred by the earlier stages, and any strict payment processes may not prevent theft.

3. Bribery and Corruption

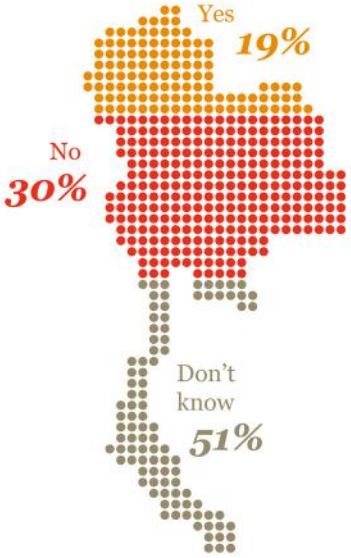
Thailand's corruption problem is endemic, with 28% of respondents reporting being asked to pay a bribe. This is significantly higher than the global and regional level of 18%, which points to a culture of corruption. Due to widespread bribery, the percentage of lost opportunities due to bribery is also higher in Thailand (24%) compared to globally (22%) and regionally (19%). But it is noted that the difference is not as large as the percentage of bribery suggests. This could mean that while bribes are commonly asked for, it is not as important a deciding factor as might be expected. This contrasts with global responses that show that bribery is less common, but more frequently translates into lost opportunities.

Does bribery and corruption cause financial loss?



Thais expect financial damage due to bribery and corruption more than global respondents, with almost half expecting losses, versus about one-third globally. This high expectation in Thailand appears to be due to the high frequency of bribe requests. However, the perceived financial losses seem to be mainly in the form of direct costs from having to pay a bribe, rather than being due to the risk of prosecution under anti-bribery legislation. We believe that as the anti-corruption regulations are enforced more often and through higher profile cases, the fear of fines, prosecution and reputational damage will also grow.

Do you expect financial losses from money laundering?

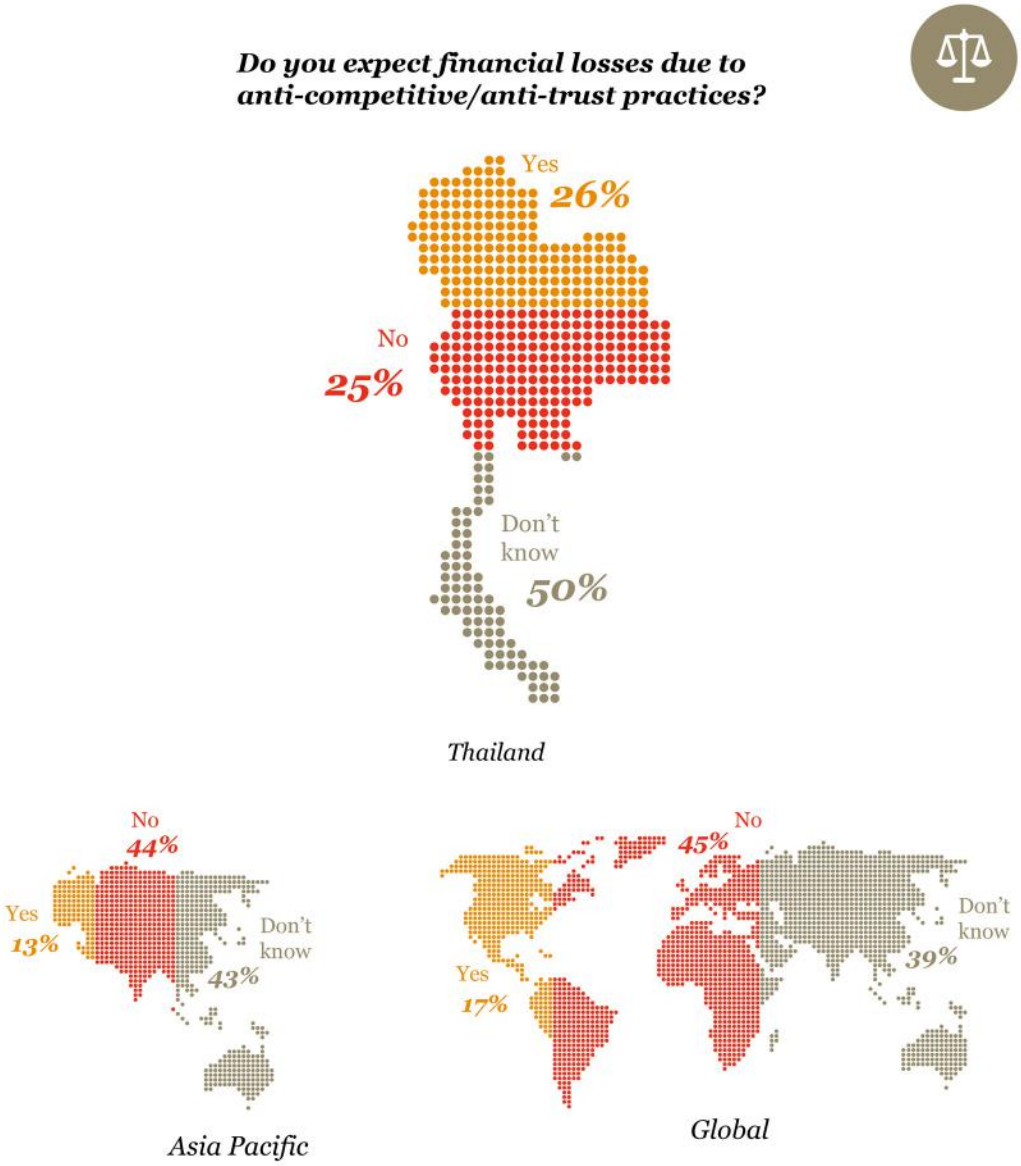


Thailand

Asia Pacific

Global

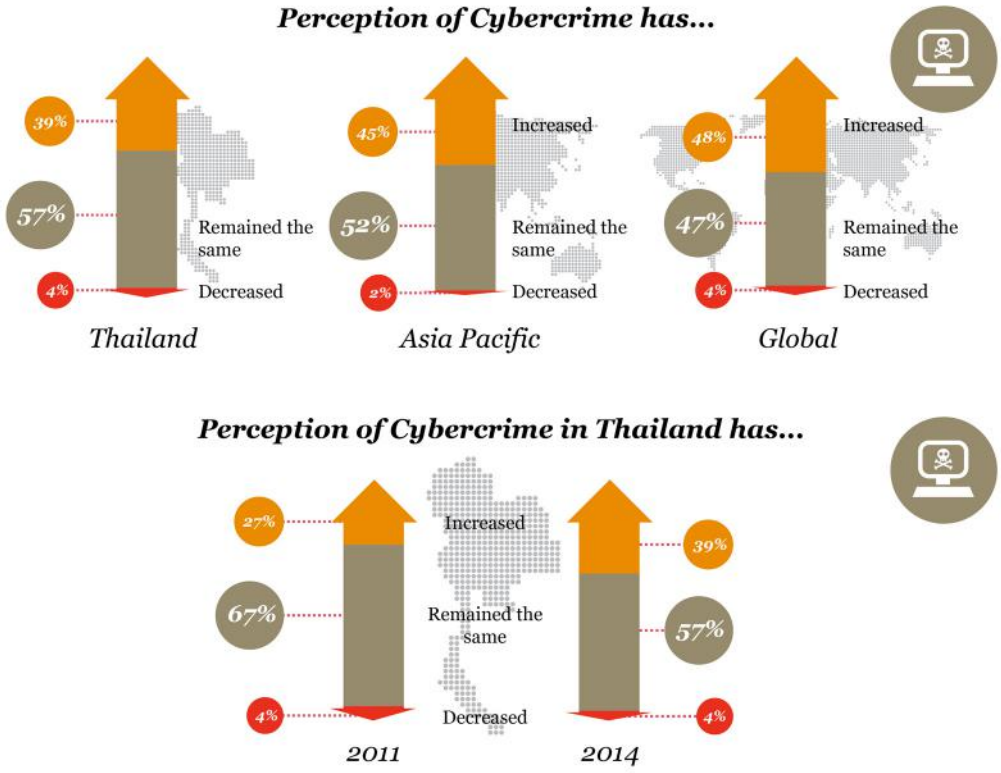
Thai respondents appeared to be much less knowledgeable about money laundering than respondents in the rest of the world, with about half replying that they "don't know" if financial damage may come from money laundering. As a contrast, only about a third of respondents world-wide gave the same answer. When they did provide a definitive answer, a greater percentage of Thai respondents (16%) expected financial damage compared to globally (10%). These responses are consistent with the lack of knowledge about money laundering in Thailand. However, we expect that with more rigorous enforcement of anti-money laundering rules in Thailand, there will be a gradual increase in the amount of awareness in Thailand. Quite often, money laundering cases here happened through illegal personal loan scheme resulted from funds derived from fraud.



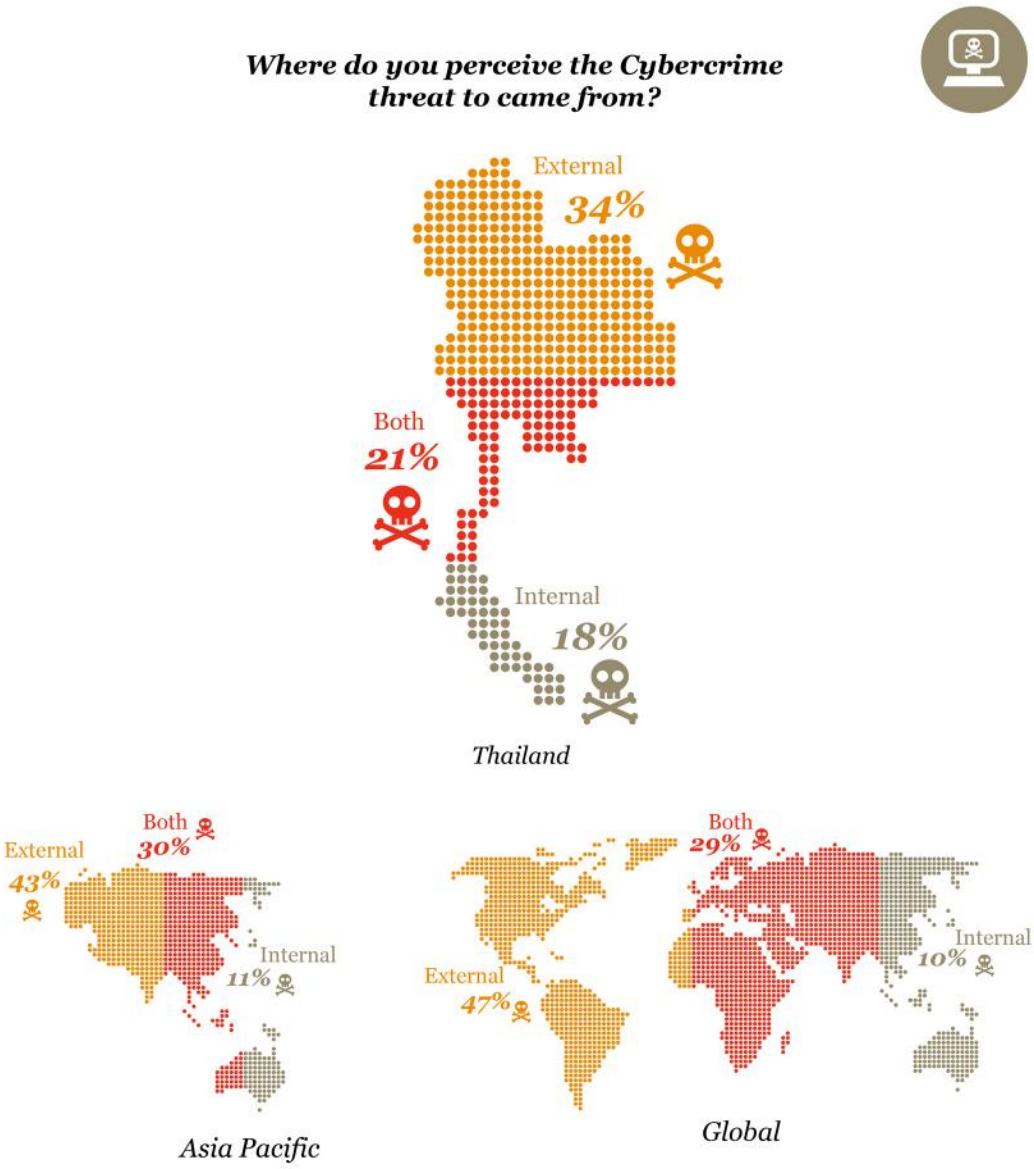
The survey found a low level of knowledge of anti-trust rules in Thailand. This is not surprising because anti-trust regulations are not strictly enforced in Thailand compared to Western countries. Also, neither the public nor the private sector see this issue as a priority.

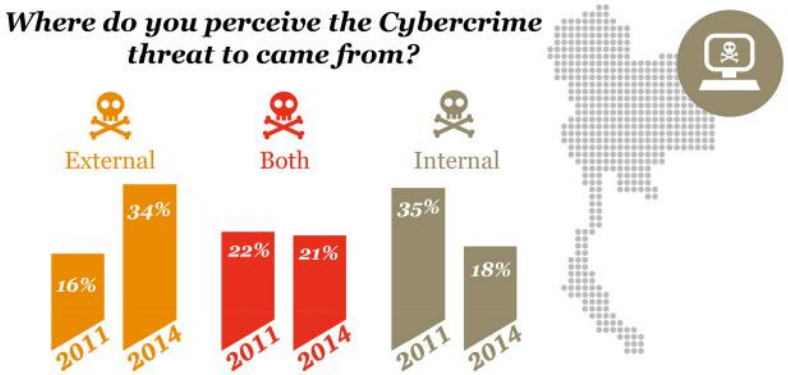
Thailand is much lower than the regional average in terms of cybercrime awareness

4. Cybercrime



The survey found that Thailand is much lower than the regional average in terms of cybercrime awareness. In turn, the regional average is much lower than the global average. However, the results of 39% are actually a great improvement on 2011 when only 27% were aware of cybercrime. The increase in perception is probably due to the increased exposure of the general populace to technology, and more coverage of the issue in the mass media.





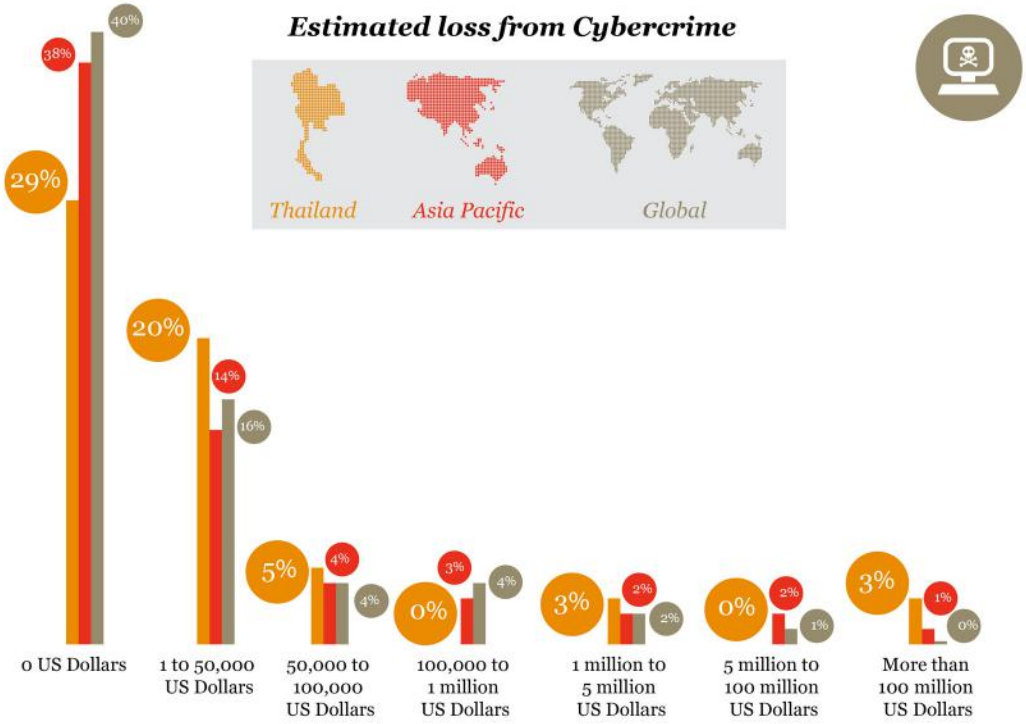
Thailand and the Asia Pacific are catching up with the rest of the world in terms how the origins of the cybercrime threat are seen. Almost half of respondents world-wide believed the cybercrime threat will come from outside, and only a tenth believed that it will originate from within. Although Thailand still sees the outside threat as less relevant, the number of respondents viewing this as the primary threat has doubled, in a dramatic turnaround from 2011. Three years ago, 16% of Thai respondents believed that the cybercrime will come from outside and 35% from inside sources. This year, however, 34% believed it would come from outside and 18% from inside. This is a complete reversal of trends.

An improved understanding of what constitutes cybercrime might be behind this change. A key component of cybercrime is an unauthorised individual who accesses information through the network. A crime that just involves a computer cannot always be classed as cybercrime. For example, a staff member selling data taken from his own company computer may not be cybercrime.

The increase in awareness of outside threats may be due to many businesses having a growing presence online. Other factors might include a number of serious fraud cases in the previous year and public awareness campaigns by local banks. For example, many banks in Thailand that offer online banking for their customers began inserting splash screens to warn their customer about counterfeit websites and other suspicious ploys to get their information. This appears to have had its desired effect of educating the public about the growing threat of cyber fraud. As more companies take their business online, the fear of outside threat inevitably rises.

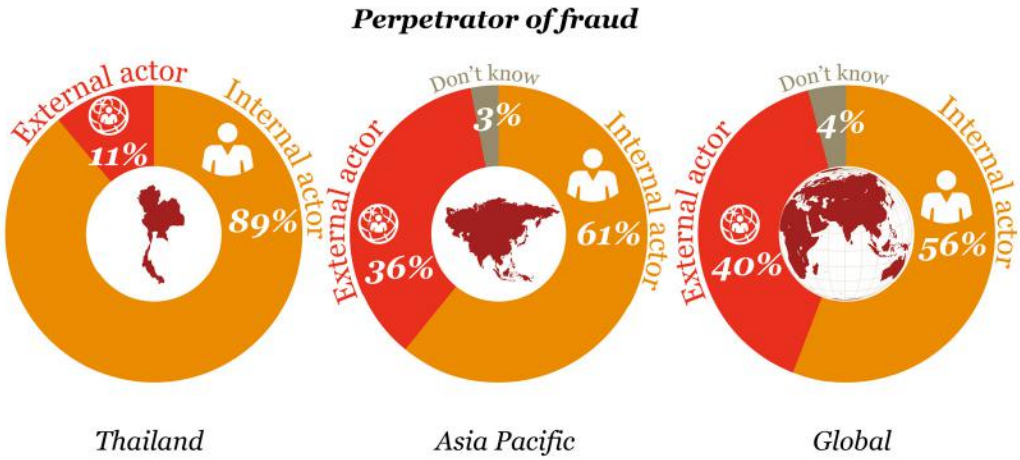
Companies are also outsourcing their email and data storage functions to cloud servers rather than maintaining in-house email servers. As connectivity and confidence in online security grows, organisational risk to external hackers has also increased. Respondents state that the cost savings and increased efficiency of cloud servers exposes their data to web-based threats of data theft and financial crime. Because this technology is so new, organisations have not yet developed policies and measures to prevent risks associated with cloud servers. We expect that this will be an increasingly important issue in the coming years.

The more 'traditional' cybercrime threats are generating higher losses in Thailand, particularly in the finance sector. Based on Thai respondents' own estimates, at least 20% have suffered proven financial damages of less than 50,000 USD. However, at least one respondent reported damages over 100 million USD. World-wide or regionally, the percentage of those who have not suffered loss from cybercrime is higher, which may correspond with greater awareness and better prevention of cybercrime abroad. But many of the cybercrime cases in Thailand have been very sophisticated and so difficult to detect. We think that the true scope of this type of fraud is greater than the numbers show.

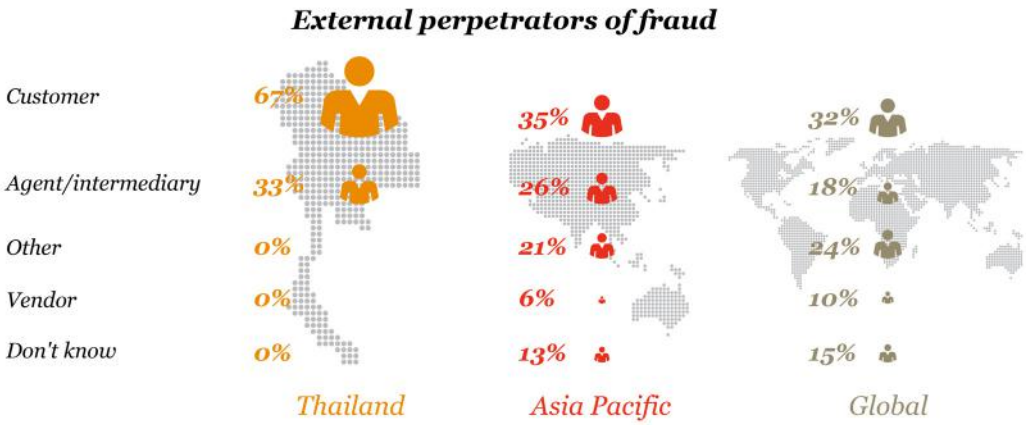


Fraud in Thailand is almost entirely carried out by insiders

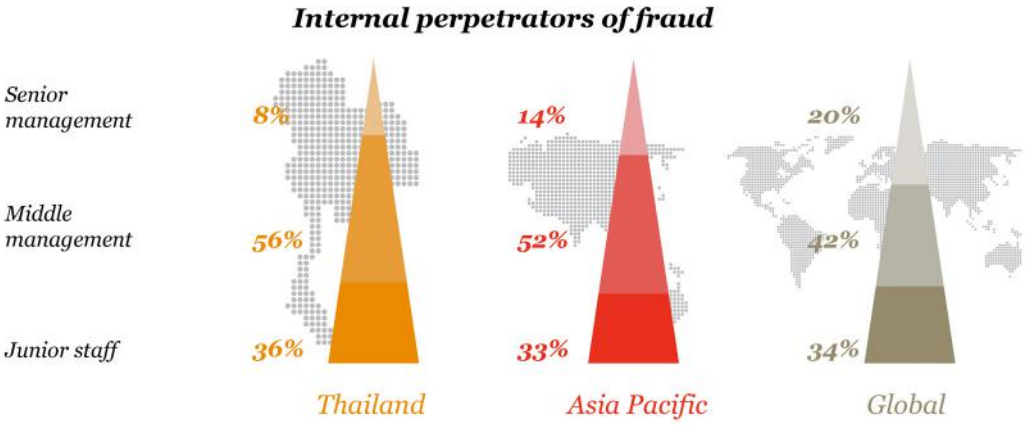
5. Perpetrators

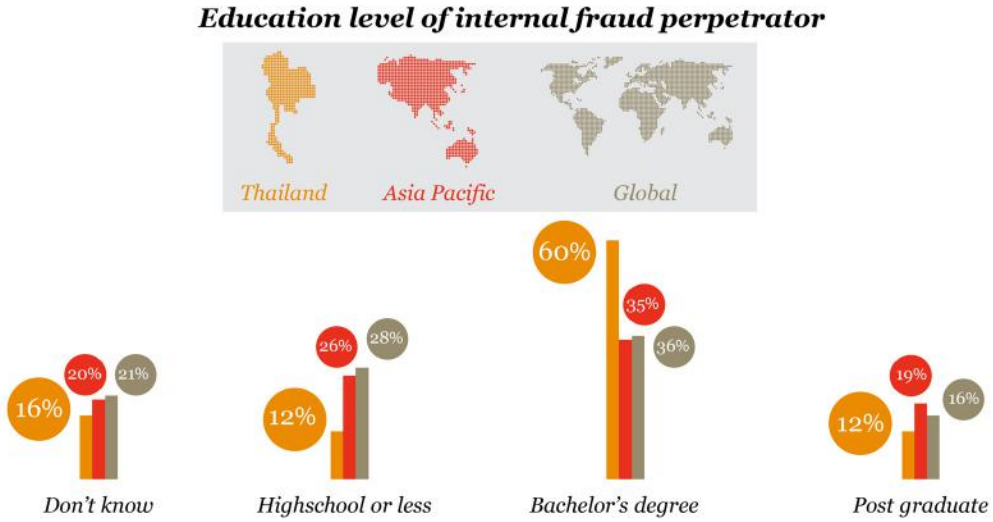


Fraud in Thailand is almost entirely carried out by insiders, according to 89% of respondents. Compared to 56% globally, this points to a level of internal fraud that is surprisingly higher than the global norm. This result may be due to weak internal controls, lack of whistle blowing mechanisms or how differently Thai respondents consider what is fraud. Additionally, it can be due to a culture of trust in Thailand. Helping one another is a common value in Thai society, but this can be a risk for companies if insufficient controls are in place. A final factor that has contributed to internal fraud is that Thailand has a large number of foreign manufacturers operating with very little supervision from head office. This opens up opportunities for theft, collusion and bid rigging by local management teams. This can easily hide their activities from foreign managers who are short on Thai language skills and local experience.



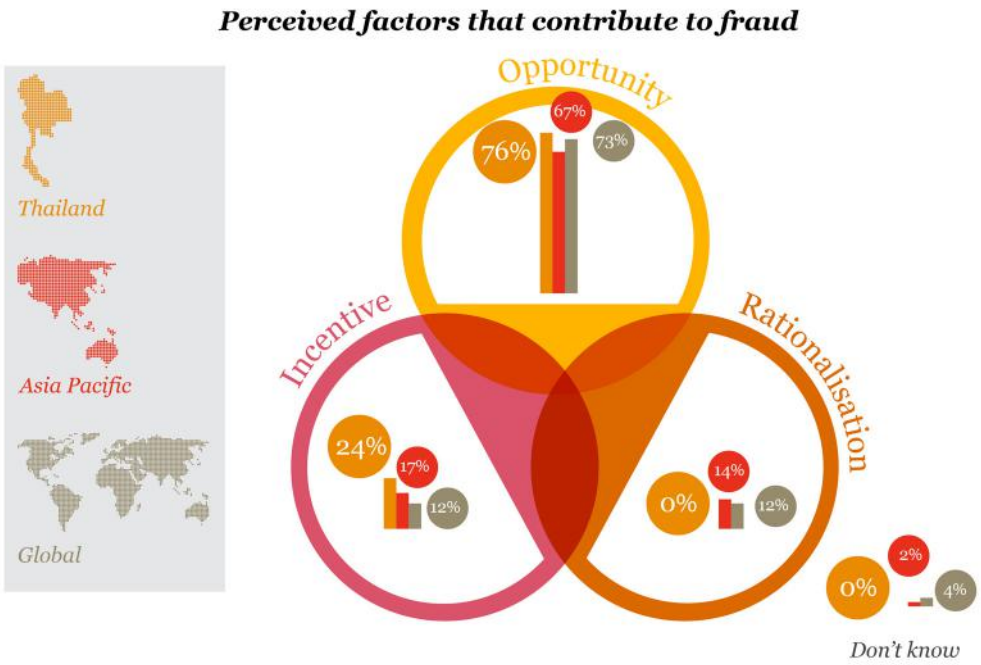
Thai respondents often had a much different concept of fraud when it was perpetrated by outside parties. Thai respondents often did not report vendors as fraud perpetrators even though the survey showed a very high percentage of procurement fraud. This suggests that Thai respondents may see procurement fraud as a one-sided act carried out by employees alone, and do not think of vendor involvement as fraud. They may even see vendor attempts to get higher profits as a normal part of business. This attitude could cause problems because dishonest vendors could be allowed to continue to do business.





The highest-risk internal employees involved in fraud are clearly middle managers who have worked at the company for between three and five years, and have a bachelor's or master's degree. Those in middle management with more senior positions have more chances to carry out fraud. This is due to their level of power and authorisation. They tend to have a strong understanding of their organisation and a high amount of access to system information. They have regular access to senior management and therefore can cause a significant amount of damage to a company. A strong sense of seniority in Thailand and Asia also affects this, which makes it less likely for junior employees to report frauds or other illegal activity to senior management. While risks in middle management can be reduced by strong controls, risks from senior management, whose personnel can operate outside normal controls, is best dealt with by better governance and increased transparency. Whistle blowing programmes are one such tool that helps prevent senior management fraud because it gives an anonymous vehicle for lower level employees to communicate wrong-doing.

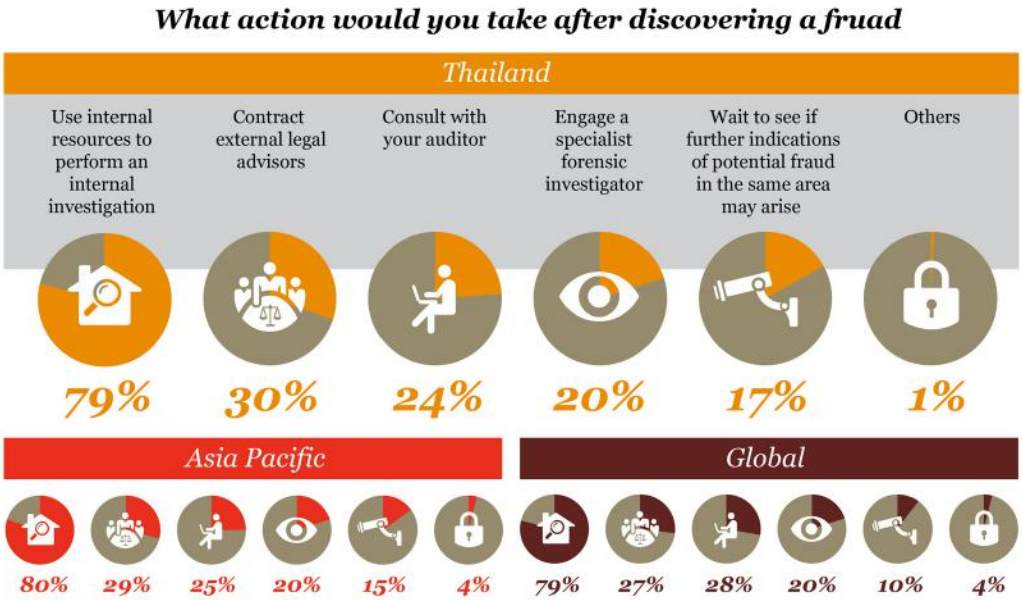
Inside perpetrators in Thailand are by a large margin, male college graduates with 3-5 years experience. Thailand is unusual in this way because globally, while perpetrators were mostly male, their education level, length of service, and management level varied quite a bit. This may reflect the employee demographic in Thailand, and the value placed on formal education. These statistics suggest that those with a formal education are much likelier to be put into high-risk positions, and so have more chance to commit fraud.



The survey asked respondents about what factors motivated perpetrators to commit fraud and found that rationalisation played a small role compared to opportunity and incentive. In the field of forensics, there is the well-accepted concept of the 'fraud triangle'. This states that fraud happens when three factors arise at the same time: a chance to commit a crime, a strong enough incentive or pressure to commit the act, and a belief that the act can be justified. This last factor, also known as rationalisation, explains that normal people, even when under great pressure, do not like to see themselves as criminals. Therefore, unless they can explain their act as non-criminal, they won't commit the crime. Rationalisation often happens due to simmering discontent or resentment against the company, such as thinking: "I am underpaid already, so it is not wrong for me to take a little bit of company cash home". This factor of rationalisation may lead to fraud if the other two factors of opportunity and incentive make it possible.

For example, a cash clerk that would not normally steal money may carry out fraud if he is underpaid, his supervisor doesn't count cash properly, and the clerk is under pressure to pay rent.

In this survey, Thai respondents do not see rationalisation as a factor that contributes to fraud. This shows a very different idea of what contributes to fraud, and means that organisations in Thailand must put into place locally-tailored prevention mechanisms. In countries where rationalisation is a contributing factor to fraud, organisations can focus on human resources and building good will as a way of reducing the motivation to commit fraud. However, in Thailand where the main motivator is opportunity, then preventing fraud becomes more a question of tightening controls, rules and overseeing processes to create a disincentive for employees to commit fraud.



Thai respondents tend to respond to fraud detection similarly to others worldwide. Eighty-percent of all respondents respond with internal actions, while a third seek external legal advice. The main difference is that Thai respondents tend to wait to see if additional frauds may take place. But being in line with the global response does not necessarily suggest that this is the best practice. Using internal resources is preferred because it is potentially cheaper, and keeps the problem 'in-house', reducing the risk of public exposure. However, internal resources may not be enough to resolve cases and it may be advisable to engage a specialist forensic investigator.

Thailand is comparatively lenient toward internal fraud perpetrators when compared to the rest of the world. Thai respondents reported a lower percentage of tough and final punitive actions, which includes dismissal, informing law enforcement, taking civil action, and notifying relevant authorities. Instead, the only category where Thailand reported a higher percentage than global or regional levels is 'warnings and reprimands', which means that perpetrators can continue to work within the organisation. This tendency to forgive may have contributed to a higher percentage of internal fraud. Interestingly, asking the fraudster to voluntarily resign from the company is a common practice here.

Despite this, the correct action for each case changes based on the company itself, the severity of the fraud, and the perceived consequences of taking action. For example, dismissal may appear to end the problem, but taking legal action carries a higher chance of getting back the lost property or funds. In some industries, dismissed employees can easily gain new positions at other companies and re-offend at future workplaces. Without good communication with other companies, fraudsters can remain in the industry and can cause damage elsewhere. Taking legal action is advised in many cases, but companies have to understand that the legal process can take time. Warnings and reprimands can have benefits in less serious cases. Forgiven employees can turn over a new leaf, and remain productive members of the company.

Contact

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

www.pwc.com/th