PwC's Global Economic Crime and Fraud Survey 2022 - Thailand Report

Protecting the perimeter: The rise of external fraud

pwc

Overview

The COVID-19 pandemic has drastically changed the business landscape. Travel restrictions mean many employees are working from home and accessing company assets remotely, while consumers are moving toward digital channels at a rapid pace. Fraud and economic/financial crime has changed at an even faster pace. Fraudsters are becoming more sophisticated than ever. The risk of cybercrime is on the rise, as well as emerging threats such as ESG reporting fraud, supply chain fraud and anti-embargo fraud.

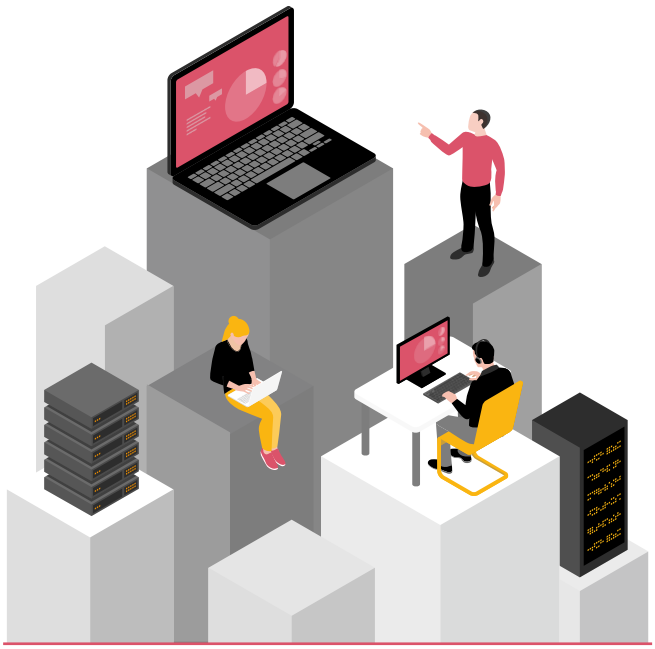
PwC's Thailand Economic Crime and Fraud Survey 2022 collected responses from over 50 Thai and multinational companies operating in Thailand (referred to as 'Thai companies' in this report) on fraud and economic/financial crime they have experienced in the past 24 months. The report outlines the current fraud landscape in Thailand as compared to the global situation. This will help Thai companies understand the trends, areas of risk, and emerging threats of fraud and economic/financial crime.

The key point is that fraud and economic/financial crime is a constantly evolving threat. Companies must periodically assess their risks and vulnerabilities, putting appropriate controls and tools in place, so that they can monitor, prevent, and respond to fraud incidents quickly and efficiently.

Thailand's Fraud Landscape

Nearly one in four (22%) of Thai companies that responded to PwC's Thailand Economic Crime and Fraud Survey 2022 experienced fraud, corruption, or other economic/financial crime within the last 24 months. It does not necessarily mean more fraud was prevented, but rather, it could indicate that more fraud has gone unnoticed. As nearly half (46%) of companies globally reported being victims in this year's survey, PwC believes fraudsters are winning the war by evolving their methods and using new technologies to breach defences undetected.

In terms of enterprise risk and compliance programmes, Thai respondents are still below global standard. Only 37% have a designated risk management/compliance function for responding to fraud risks (compared to 43% globally). Moreover, in the past 24 months, less than 30% of Thai respondents have increased the size of enterprise risk management/compliance functions (compared to 53% globally). This indicates that, globally, companies are increasing the focus and investment on risk and compliance functions to protect themselves from fraud and economic crime. However, Thailand is falling behind in this aspect.



Compared to

43% global

37%

have a designated risk management/compliance function for responding to fraud risks

Compared to

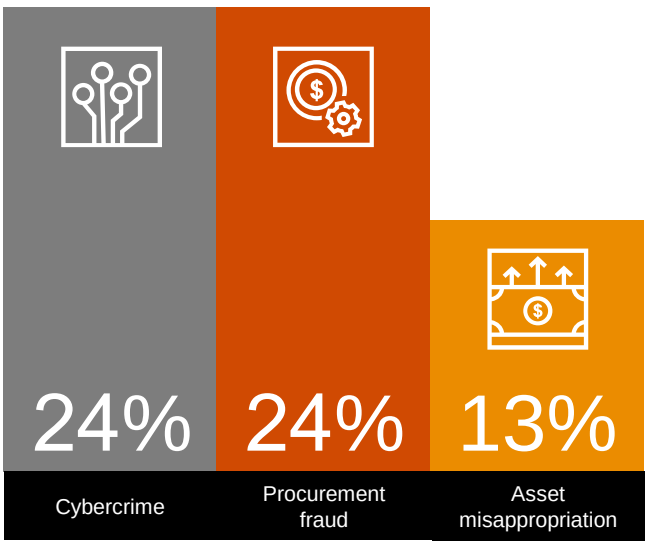
53% global

Less than

30%

of Thai respondents have increased the size of enterprise risk management/ compliance functions

As a result of the disruption caused by the COVID-19 pandemic, Thai companies experienced the highest increased risk in cybercrime (24%), procurement fraud (24%) and asset misappropriation (13%).



It is not surprising that procurement fraud and asset misappropriation are near the top of the list for Thailand as 41% of the survey respondents were from industrial products and manufacturing industry where these types of frauds are known to be prevalent. These two fraud types were among the top fraud risk stated by Thai companies in the 2018 and 2020 surveys.

The rise of cybercrime is expected as COVID-19 caused companies to permit access to their assets remotely while employees work from home. Among Thai respondents, cybercrime risk rose from only 16% in the 2020 survey to 24% in 2022. This view is shared across almost all industries and countries where nearly one-third (29%) of companies globally experienced an increased cybercrime risk.

Organised crime groups can recruit more easily during an economic downturn, bringing in new members who are suddenly unemployed. As a result, they are becoming more specialised and professional, with goals, incentives and bonus structures. They take advantage of vulnerabilities and invest continuously to outsmart their prey. Their attacks are becoming more complex, and include the dark web, cryptocurrency, data breach specialists, synthetic/false ID creation, new attacking methods, and other areas that allow organised crime groups to connect, coordinate, and transact within a growing criminal economy.

The nature of the risk is borderless. Hackers can initiate cyber-attacks from anywhere in the world and request ransom payments be made through international channels such as cryptocurrency. Cyber-attacks tend to be immune to traditional prevention tools such as codes of conduct, investigations or training. PwC believes the increased frequency of cyber-attacks will undoubtedly continue and companies will need strategies to protect themselves from fraudsters.

Emerging threats

Emerging risks are risks that are relatively low on the radar but have the potential to cause greater disruption in the next few years. The challenge with managing emerging risks is that companies may fall into the trap of only seeing what is known and not seeing what is unknown. Then as the emerging risk starts to rise, companies may suddenly find themselves in the position of not being sufficiently prepared to handle the risks. So, it is important to identify and closely monitor emerging risks to prepare and respond quickly and appropriately. Based on the current outlook, PwC believes at least the three following areas should be on the radar.

Anti-embargo fraud

Just

6%

of companies globally (and no Thai respondents) said they experienced anti-embargo fraud in the last 24 months.

But this is very likely to change in the next 24 months as global sanctions rise to the highest levels in recent history due to trade war and the sanctions against Russia for Ukraine invasion.

Supply chain fraud

Globally, one in eight companies experienced incidents of supply chain fraud as a result of the disruption caused by COVID-19. One in five sees supply chain fraud as an increased risk as a result of the pandemic, although, for Thai respondents, only one in ten feels that way.

Although the number seems to be relatively low, recent months have seen increasing supply chain shortages at a global level. This does have a direct impact on companies' vulnerability to fraud.

90%

of Thai survey respondents **have the most extensive impact from lacking risk** visibility throughout the supply chain.

Insufficient technology/processes and a lack of staff to identify and manage supply chain risks are also the following key areas which are correlated to supply chain fraud. Pandemic countermeasures have forced manufacturers to comply with sudden changes of regulations, specifically on operating hours and labour management.

As Thailand is considered a critical manufacturing hub, the importance of potential risks associated with the supply chain cannot be overlooked. Consequently, Thai respondents have been conducting various activities such as staff training and risk assessment, enhancing compliance programmes, and identifying staff responsible for managing supply chain risks.

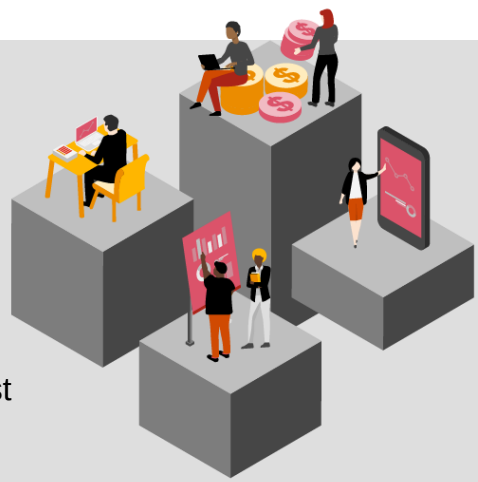
As less than

10%

of Thai respondents are proactively **monitoring supply chain risks, the ability to identify fraud/misconduct within the supply chain is relatively low,** making this an excellent target for fraud.

ESG reporting fraud
Trust has become a key lever for value creation. PwC's 25th Annual Global CEO Survey highlighted the relationship between companies with a high level of trust and their ability to drive change. But trust is fragile. A perceived or real misstep in transparency can wreak havoc on brand reputation and underlying trust.

With environmental, social and governance (ESG) responsibility growing in importance to stakeholders, accuracy in ESG reporting is essential.



Globally, just

8%

of organisations encountering fraud in the last 24 months experienced **ESG reporting fraud** (none for Thai respondents) but the incentive to commit fraud in this area is only going to increase – as will the consequences.

Although **more than half of Thai respondents** have processes to identify and manage potential ESG risks; the manipulation of ESG reports either by employees or third parties are still their key concerns. While adding investment in people and technology would further strengthen risk management capabilities, it is fundamentally necessary to increase ESG awareness within companies with clearly defined ESG objectives, as well as result tracking and monitoring.

Conclusion

Apart from conducting a health check exercise, known as a periodic fraud risk assessment, to understand how key fraud risks are being proactively monitored, with external fraud growing, there are three considerations to help strengthen your fraud risk management:

1

Understand the end-to-end life cycle of customer-facing products. Take the time to identify where opportunities exist for a fraudster to exploit a product and cause financial, legal or reputational damage. How could it happen, what would it take to prevent it from happening, and what type of response is needed if it happens?

2

Strike the proper balance between user experience and fraud controls. Protecting customer-facing channels will require a delicate balance between ensuring that users have a great experience and detecting and stopping fraudsters. The dual objectives of keeping false positives as low as possible and catching true fraud can be achieved through a combination of fraud technology, strategy and processes.

3

Orchestrate data. Often, fraud signals will come from disparate, disconnected systems and are only detectable through the occasional manual review. It is crucial that fraud indicators are orchestrated into a centralised platform that can track the end-to-end life cycle of users (fraudsters or not) and generate meaningful alerts.

Preventing fraud and economic crimes is a complex challenge. It takes continuous improvement in governance, people, processes, and the use of sophisticated technology to protect the perimeter and combat formidable bad actors who are becoming better and better at exploiting the cracks.

Get in touch

Phansak Sethsathira
Risk Consulting Partner
PwC Thailand
Tel: +66 (0) 2844 1000 ext. 1043
Email: phansak.sethsathira@pwc.com

www.pwc.com/th