www.pwc.com/th

Thailand Economic Crime Survey 2011

Cybercrime: are you at risk?

pwc

Contents

Forewords

Thailand Economic Crime Survey 2011

Cybercrime: Are you at risk?

Globally, many companies rely heavily on the internet for many key functions from marketing and selling their products, to conducting day-to-day communications. This emerging trend is catching on in Thailand. While the internet is creating unprecedented opportunities for many Thai companies, it is also catching many of them unprepared, exposing them to risks perpetrated by disgruntled workers in their own offices; or seasoned cyber criminals in other parts of the world.

Companies worldwide are losing billions of dollars to economic criminals, and suffering incalculable damage to their reputations, both with their customers and the public at large. In our first-ever economic crime survey in Thailand, more than one-third of respondents reported being the victim of economic crime in the past year, with 64% of these stating they have lost up to 3 million baht. Perhaps most concerning is that nearly 80% of economic crime in Thailand was perpetrated by internal sources, such as employees.

PwC's experience has taught us that economic crime is truly global and that no industry or organisation is immune. However, our survey found that the threats and responses to cybercrime differ from country to country and that some industries are more prone to cybercrime than others. In Thailand's case, companies tend to pay too little attention and effort to fraud-prevention activities such as fraud risk assessments or control and monitoring systems that can automate fraud detection. This makes Thai companies much more vulnerable to increasingly sophisticated cyber criminals looking to take advantage of internal weaknesses and limited oversights.

We hope our report will help your firm to equip your people, process, and technology with sufficient capability to fight against this growing challenge.

Sira Intarakumthornchai
Chief Executive Officer, PwC Thailand

Rising trend in complex economic crime

Thailand's rapid growth in recent years presents unique opportunities for many organisations, both global and local Thai entities, and this first-ever Thailand edition of PwC economic crime survey results show that along with these opportunities, come risks. The growing economy means more competition and rising expectations from management, which adversely places immense pressure on middle managers to meet soaring targets. In some cases, this can contribute to corner-cutting to meet these expectations. Companies therefore run the risk of losing oversight of the processes and controls that mitigate them from both internal and external threats.

This survey provides an unbiased insight into the types of fraud and misconduct that are prevalent here in Thailand. The results also represent a snapshot of the types of fraud cases that PwC Forensics team in Thailand are actively involved with on a day-to-day basis and demonstrate the mounting challenges facing organisations operating here. As a local practitioner in corporate investigations, I have seen a rising trend in complex embezzlement, corruption and IT related crime, which costs companies hundreds of millions of baht in direct losses, let alone the wider impact to these organisations. However, this has gone hand-in-hand with an increasing interest among large corporations in initiating fraud prevention and detection mechanisms. I also observe that the concept of forensic accounting and fraud examination is also being well received in academic institutions, which is a welcoming sign.

Therefore, the information contained in this report can be an invaluable tool to educate business leaders and the public about the widening spectrum of threats posed by economic crime. I hope that the survey will help your organisation to equip itself to meet these challenges.

Vorapong Sutanont
Partner, Forensic Services, PwC Thailand

Executive Summary

Economic crime continues to be a serious issue affecting organisations worldwide. No industry is immune. The global costs run into the billions, not to mention the remedial and collateral damage that can strike an organisation to its core. The effects can seriously damage a brand, leading to significant loss of market share. As society becomes less tolerant of unethical conduct, businesses need to ensure that they place a premium on building public trust.

To understand and confront these issues, we are pleased to present our first Thailand Economic Crime Survey. Our 2011 survey turned the spotlight on the growing threat of cybercrime in a world where most individuals and businesses rely on the internet and associated technologies, opening themselves to the risk of attack from global criminals from anywhere. Against the backdrop of rising incidents of data loss and theft, computer viruses and hacking, the survey scrutinised the significance and impact of this emerging type of economic crime and the way it affects business worldwide. A set of questions was asked specifically relating to cybercrime, including the threat posed by cybercrime and how organisations are protecting themselves. To enable us to determine long-term cybercrime trends, respondents were asked a number of 'core' questions on economic crime.

The 2011 Thailand Economic Crime Survey was completed by 79 respondents from various industries in Thailand. Of the total respondents, 39% were of C-suite/Senior Executive level, 38% represented listed companies, 44% are multinational corporations, and 32% represented companies with more than 1,000 employees. The feedback from this wide range of respondents allowed us to conduct deep analyses of the data and compare it with previous surveys to establish trends and developments.

The survey found that 35% of our Thai respondents have suffered from one or more types of economic crime in the past 12 months. This result is consistent with the 34% from global result and 31% from Asia Pacific region. Of those from Thailand, 7% said they had been victims of cybercrime in the past 12 months and almost half of all respondents noted an increasing awareness of cybercrime threats.

This year's Thailand report is divided into two sections:

- Cybercrime – how it impacts organisations, their awareness of the crime and what actions they are taking to combat the risks; and
- The current fraud environment – focussing on the types of fraud, how it is detected, who is committing it and the repercussions.

Cybercrime in the spotlight

In PwC's view, there are five main types of cyber attack, each with its own distinct – though sometimes overlapping – methods and objectives. They are:

- ***Financial crime and fraud*** – This involves often highly organised and well-funded criminals using technology to steal money and other assets.
- ***Espionage*** – Today, an organisation's valuable intellectual property (IP) includes corporate electronic communications and files as well as traditional IP such as research and development (R&D). IP theft is a persistent threat and the victims may be unaware until knock-off products suddenly appear on the market, or a patent based on their R&D is registered by another company.
- ***Warfare*** – This can take place between states, or may involve states attacking private sector organisations, especially critical national infrastructure (CNI) such as power, telecoms and financial systems.
- ***Terrorism*** – This threat overlaps with warfare. Attacks are undertaken by terrorist groups (possibly state-backed), again targeting either state or private assets, often CNI.
- ***Activism*** – These attacks are undertaken by supporters of idealistic causes – most recently the supporters of WikiLeaks.

The 2011 Global Economic Crime Survey (GECS) focused on the financial crime and fraud aspect of cybercrime and for the purposes of our survey questionnaire, cybercrime was defined as follows:

"Cybercrime, also known as computer crime, is an economic offence committed using the computer and internet. Typical instances of cybercrime are the distribution of viruses, illegal downloads of media, phishing and pharming and theft of personal information such as bank account details. This excludes routine fraud whereby a computer has been used as a by-product in order to create the fraud and only includes such economic crimes where computer, Internet or use of electronic media and devices is the main element and not an incidental one". [1]

Cybercrime can range from an orchestrated attack on a company network, to a sales executive who extracts key sales and marketing data from his previous employer by saving documents onto a USB stick, or transferring confidential files via email prior to taking up employment with a competitor

So, is cybercrime simply a means by which a fraudster commits the illegal act, or is it an economic crime in its own right? Should organisations take specific measures, over and above other fraud prevention and detection methods, to manage this risk? Our 2011 survey takes a closer look.

[1] As defined in GECS 2011 by PwC in conjunction with our survey academic partner, Professor Peter Sommer.

Cybercrime enters the frame

Our 2011 global survey ranked cybercrime as one of the top four economic crimes behind asset misappropriation, bribery and corruption, and accounting fraud. This trend is consistent with the result from Asia Pacific survey. Although it is not yet recognised as a prevalent threat in Thailand, our findings suggest the threat is escalating and that economic crime is fast becoming a prime concern among decision makers. [See figure 1]

With internet penetration rates growing at double-digit rates, cybercrime has become a major focus for our clients and partners. We focused on cybercrime this year to raise awareness of the growing threats posed to businesses and government institutions and to illustrate the opportunities. Therefore, we reintroduced it in the 'types of fraud' question, asking the respondents whether they had experienced cybercrime in the past 12 months.

Figure 1: Top four types of economic crime reported globally

% respondents who experienced economic crime in the last 12 month

So how and why has cybercrime emerged as one of the top forms of fraud? Our research found the reasons are:

- Increased media attention on the Computer Crime Act of 2007, leading to a heightened awareness of cyber fraud, and causing organisations to implement extra controls to detect and report economic crime;
- Reclassification of traditional economic crimes as cybercrime because these were committed by using a computer, electronic devices or the internet;
- The growth of online banking, which has made consumers and organisations vulnerable to worms, trojans and viruses; and
- A boom in social media as a means for Thai companies to communicate with clients. Many companies still lack monitoring and usage policies to protect from cybercrime.

Regardless of the reasons, ***27%*** of economic crime victims in the last 12 months indicated that they perceive the risks of cybercrime to be on the rise while ***67%*** of the victims believe that the risks of cybercrime remains the same. Only ***6%*** believe that the risks are subsiding and the remainder believe the risk of cybercrime will remain at the same level. Our findings clearly indicate that cybercrime is an emerging threat and of great concern.

The risk and reward matrix of cybercrime

The dynamics of cybercrime are different from other conventional economic crimes. It can have a range of different motives including financial gain, competitive advantage, testing one's technology skills or curiosity. We have analysed and evaluated the incentives and opportunities attached to cybercrime compared to other conventional economic crimes and found that it can offer a different risk and reward matrix than conventional economic crimes.

Take for example an armed bank robbery. The perpetrator takes a number of significant risks in order to carry out the crime:

- Physical presence at the site. This creates the risk of being caught in the act. Other deterrents such as closed circuit television cameras and security alarm systems heighten the risks;
- A perpetrator armed with a lethal weapon may cause injury or death, meaning the perpetrator could face additional criminal charges, such as murder or manslaughter;
- Conversely, a cybercriminal that infiltrates a banking system remotely to steal funds, customer bank details or personal information takes on fewer risks;
- The crime can be committed from anywhere and at any time – meaning the perpetrator does not need to be physically present at the site, which reduces the risk of being caught;
- The perpetrator does not need to be armed with weapons to perform the act and is unlikely to cause physical harm to others.

There is less chance of law enforcement being able to identify the perpetrator or determine their location. More often than not, the perpetrator is located outside of the country in which the target is based, making it difficult to apprehend and prosecute. In addition, current laws are not mature enough to effectively prosecute cyber criminals. Technological advancements are fast, which greatly influences cybercrime – to the extent that legislation and corporate policies need to be continually assessed and monitored to ensure that they keep track;

Geographic, law enforcement and political obstacles mean that the perpetrators can continue to 'return to the scene of the crime' with minimal fear of detection.

While robust preventive measures can mitigate the risk of traditional economic crime such as asset misappropriation, bribery and corruption, and accounting fraud, rapid technology change makes it difficult for organisations to keep up with cybercrime.

Is cybercrime really an external threat?

As the population becomes more tech savvy, organisations face ever-increasing internal threats from employees and related parties. Whereas a decade ago, faceless external hackers were seen as the only threat, today respondents see a growing trend of internal cybercrime. Our research shows that ***35%*** of respondents believe that cybercrime is home grown. However, another ***22%*** of all respondents see this as both an external and/or an internal threat. This suggests that the perception of cybercrime is changing from being an exclusively external threat to an internal one, and organisations are now recognising the internal risks from cybercrime.

For Thai respondents who indicated that the threat of cybercrime came from within their organisation, ***49%*** thought that the information technology (IT) department was the most likely source. It is not surprising that many respondents consider the IT department's personnel to be the most likely internal perpetrators, as they are expected to have the knowledge, skills, opportunity and capability to undertake such crimes. In addition, IT personnel may have 'super-user' access, which gives them additional administrative rights to access systems and delete audit trails.

Interestingly, our survey respondents recognise that cybercrime risks are not restricted to the IT department but that other areas such as Sales and Marketing ***(44%)***, Physical Information Security Department ***(31%)*** and Finance ***(18%)*** also pose risks.

The Human Resources ***(18%)*** and Legal ***(4%)*** departments were considered to be the least likely internal perpetrators; however, these departments should not be ignored as cybercrime can come from anywhere – for example, a malicious employee with access to confidential HR data or legal documents.

To illustrate, we have outlined high-risk areas for cybercrime:

- Disgruntled employees accessing HR data to extract personal information on pay and bonuses ;
- An employee accessing a colleague's emails and sending malicious emails from this account or bullying other members of staff ('cyber-bullying');
- Extracting key information from the Accounts Payable department via email, setting up dummy supplier information, and extracting funds from the company;
- Publishing sensitive information through social media or sharing information with one's 'friends' or connections while on the job.

Are these strictly cybercrimes or are they forms of economic crime where the internet is just a means to an end? Our survey shows that irrespective of ambiguity around the definition of cybercrime and what it constitutes, the threat is not just coming from the IT department but is posed by departments across the whole organisation.

Where does the external threat come from?

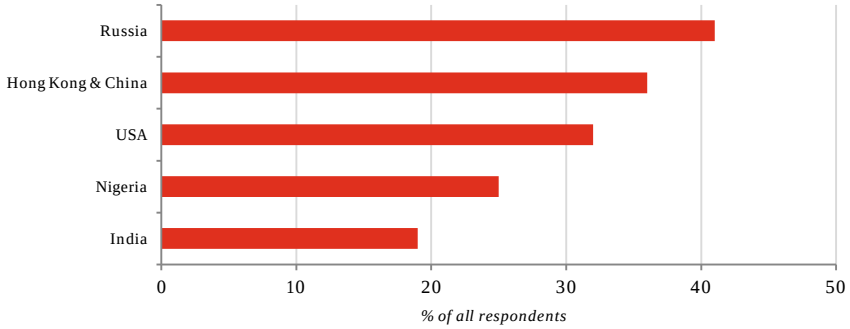
As highlighted above, many global respondents perceive cybercrime as an external threat. In this regard, we asked all respondents whether they perceived the cybercrime risk to be prevalent within their country or if it was coming from abroad. For global respondents who indicated it was a foreign threat, the following top five countries were perceived as the sources.[2] [See figure 2]

The table shows that the prevailing perception is that Russia, Hong Kong and China are the greatest cybercrime threats, as indicated by nearly **two out of five** respondents. Nigeria also ranked quite high. However, there is no evidence to suggest that Nigeria is a high-technology crime hub, but perhaps activities such as the advance fee payment scams or so-called '419' fraud, which are communicated via email (rather than by post), may be considered cybercrime. The US and India also ranked high, indicating that countries with IT-savvy populations are deemed to pose a high cybercrime threat.

This demonstrates that cybercrime can come from anywhere in the world where there is a computer, smart phone, or other electronic device able to access the internet. The cybercrime perpetrators can be organised criminals operating from multiple locations across the globe.

Similar to the black market for consumer goods, criminal exchange websites, such as DarkMarket, are emerging where stolen credit card details are sold for as little as a few cents. There is also the new form of political activism, ('hacktivism'), as illustrated by the group "Anonymous". Two recent cases include retributive hacking into major credit card companies after they withdrew support from WikiLeaks or the temporary shutdown of Sony Playstation Network due to the security breaches of over 77 million users.

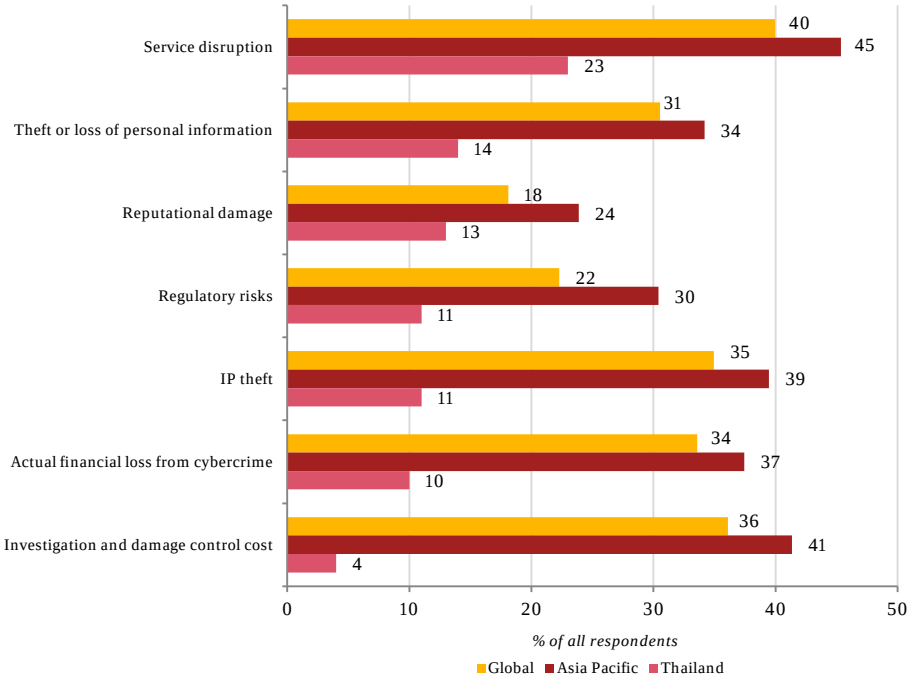
Figure 2: Top five countries perceived as origins for perpetrating cybercrime by global respondents



Is your organisation's reputation at stake?

Our survey investigated respondents' concerns about the effects of cybercrime on their organisation with regard to service disruption, theft or loss of personal data, reputational damage, regulatory risks, IP theft, financial loss, and investigation costs. Twenty-three percent of the Thai respondents are very concerned about the risk of service disruption. They were also very concerned about other risks such as theft or loss of personal data, reputational damage, regulatory risks, IP theft and financial loss. [See figure 3]

Figure 3: Concerns about cybercrime



[2] This question was asked of all respondents who indicated that the cybercrime risk was coming from outside their country or from both within and outside their country of operation.

Is your organisation like a deer in the headlights?

As we saw earlier, ***94%*** respondents who had experienced economic crime in the last 12 months said they perceive the risk of cybercrime to be growing or remaining the same. While aware of the risks, organisations are doing little about them and seem to be reactive rather than proactive about cybercrime threats.

Our survey shows:

- ***10%*** of all respondents do not know whether their organisation has in-house capabilities to prevent and detect cybercrime;
- ***63%*** do not know whether their organisation has the in-house capability to investigate cybercrime;
- ***72%*** do not have, or are not aware whether their organisation has access to internal or external forensic technology investigators;
- ***68%*** do not have, or are not aware if their organisation has a media and PR plan in place; and
- ***53%*** do not have, or are not aware whether their organisation has controlled emergency network shutdown procedures.

Monitoring social media sites

80% of respondents stated that their organisation either does not monitor the use of social media sites or that they are not aware if their organisation monitors them. This is a startling finding, as it indicates that there is a lack of awareness of the cyber security risks these sites can present.

While social media sites such as Facebook, Twitter or LinkedIn may not be the real source of cyber crime, they can be used to socially engineer cyber economic crime. For example, social media sites can be used to collect information about a targeted individual (also known as 'spear fishing'), to research staff members or install malware onto the user's computer, making the cybercrime more effective.

Of those respondents that said their organisation is taking measures to prevent the risks, most reported that this was done via monitoring electronic traffic including web pages (internal and external) ***(94%)***, followed by employee contracts referring to proper use of information and documentation ***(69%)***, and the organisation hosting training programmes ***(38%)***. This suggests that those who are taking steps to prevent and detect cybercrime are doing it right but others are exposed to huge risks, including reputational damage and loss of sensitive information.

Monitoring social media sites

80% of respondents stated that their organisation either does not monitor the use of social media sites or that they are not aware if their organisation monitors them. This is a startling finding, as it indicates that there is a lack of awareness of the cyber security risks these sites can present.

While social media sites such as Facebook, Twitter or LinkedIn may not be the real source of cyber crime, they can be used to socially engineer cyber economic crime. For example, social media sites can be used to collect information about a targeted individual (also known as 'spear fishing'), to research staff members or install malware onto the user's computer, making the cybercrime more effective.

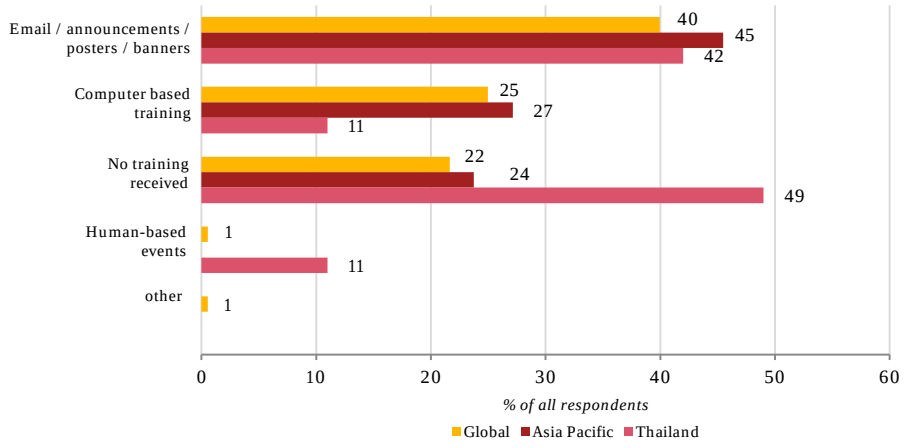
Of those respondents that said their organisation is taking measures to prevent the risks, most reported that this was done via monitoring electronic traffic including web pages (internal and external) ***(94%)***, followed by employee contracts referring to proper use of information and documentation ***(69%)***, and the organisation hosting training programmes ***(38%)***. This suggests that those who are taking steps to prevent and detect cybercrime are doing it right but others are exposed to huge risks, including reputational damage and loss of sensitive information.

Managing cybercrime risk

While our survey results indicate that cybercrime is becoming better understood, it is worrying to learn that ***49%*** of respondents in Thailand have received no cyber security training in the past 12 months, which implies that they are potentially unaware of the risks that cybercrime presents to their organisation.

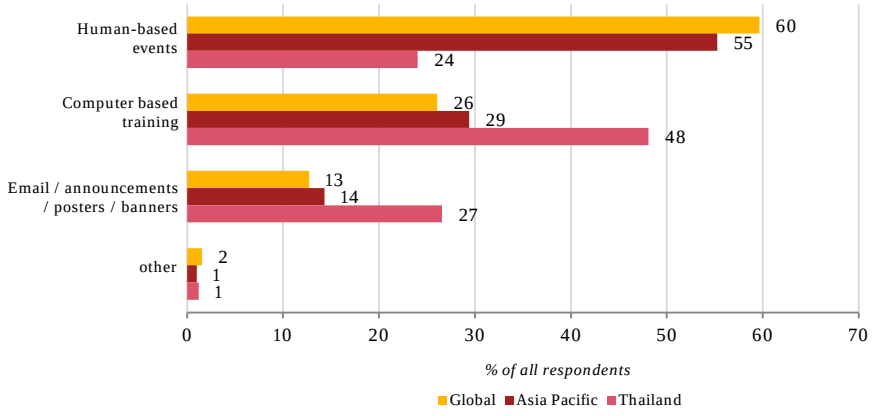
Organisations have a variety of tools to train staff and we asked respondents if they had received any training via email announcements, computer-based courses or human-based events such as presentations, team meetings and workshops. Of those who had received training, most was via non-human-based events. The survey found that 11% on Thai respondents had received computer-based training, ***42%*** of them also received email announcements and poster events and only ***11%*** received human-based training. [See figure 4]

Figure 4: Cybercrime training received in the past 12 months



Unsurprisingly, few respondents have received human-based training since it is generally considered more costly and time consuming. In light of the cutbacks within most organisations over the past 12 months, training budgets are likely to have been reduced. However, ***48%*** of respondents ranked human-based training courses as the most effective form of cybercrime training and awareness programme. [See figure 5]

Figure 5: Most effective types of cybercrime training perceived



Ultimate responsibility for managing cybercrime

Cyber security used to be pigeonholed as an IT issue, creating a communications gap between managers and security professionals. Awareness is now growing that cyber security is not only a technical issue, but a core business imperative. PwC's 2011 Global State of Information Security Survey confirms that executive recognition of security's strategic value is now becoming a core business issue, with the single most common reporting channel for chief information security officers (CISOs) now being the CEO rather than the chief information officer (CIO).

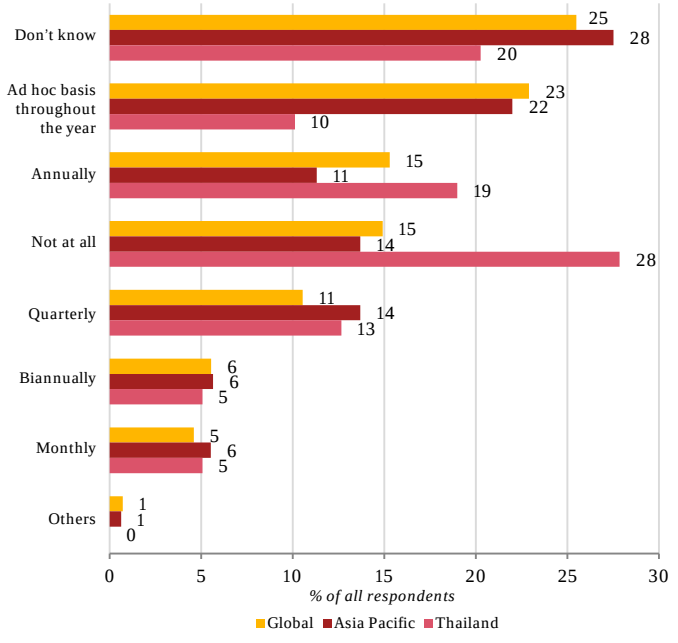
Our Thailand survey examined cybercrime from the perspective of economic crime rather than information security and we asked respondents who should ultimately own responsibility for managing cybercrime risk. The results show that ***39%*** of respondents believe that the ultimate responsibility for managing cybercrime fraud rests with the CIO. Only ***33%*** stated that ultimate responsibility resides with the CEO and the Board. This indicates that, irrespective of whether the CIO sits on the Board, responsibility is not shared with the CEO and the Board as a whole.

While we understand that the Information Technology security risk is usually the responsibility of the Chief Information Officer or the Technology Director, the expectation is that the CEO and the Board must understand and regularly investigate cybercrime risk-related matters.

Our Thailand survey found that the CEO and the Board do not perform routine reviews of cybercrime risk. ***28%*** reported that they have never reviewed these risks at all while ***10%*** of Thai respondents stated that the CEO and the Board review cybercrime related risks on an ad hoc basis. [See figure 6]

Our survey shows that the most senior people within organisations are not placing enough emphasis on managing the real threat that cybercrime fraud presents to their organisation. This is why PwC has introduced the concept of the cyber-savvy CEO. In the future, we believe that leadership by a CEO who truly understands the risks and opportunities of the cyber world will be a defining characteristic.

Figure 6: Review of cybercrime risks by the CEO and the Board



Defending against a cyber attack

1. Get the CEO involved. The CEO and Board need to be aware of cyber threats.
2. Reassess the organisation's security and cybercrime preparedness. Unlike traditional **'economic crimes'**, cybercrime is fast-paced, with new risks emerging. That means an organisation needs to constantly adapt its procedures.
3. Organisations need to have a clear awareness of their current and emerging cyber environment. If this is in place, well informed and prioritised decisions and actions can be taken.
4. Create a cyber incident response team, ready to act with speed and agility. A well-functioning cyber response team allows the organisation to pinpoint and eliminate a threat anywhere in the business.
5. Educate all employees – an organisation needs to embed a 'cyber awareness' culture, by recruiting those with the relevant skills so that this knowledge can be shared with all employees, creating a cyber-aware organisation that is better able to protect itself.
6. Take a more active and transparent stance towards cybercrime: pursue cybercriminals through legal means and publicly communicate the actions the organisation is taking.

Fraud, the fraudster and the defrauded

Fraud – what are we facing?

Over one-third of companies are hit by economic crime

Fraud continues to threaten Thai companies, with ***35%*** of respondents reporting economic crime in their organisation in the previous year and ***11%*** saying they don't know whether economic crime existed in their firm. These findings were consistent with responses from other regions. [See figure 7]

Most common types of crime

Link in other countries, Thai respondents identified asset misappropriation as the most common type of economic crime. Bribery and corruption and anti-competitive behaviour are significantly higher in Thailand than in other jurisdictions. [See figure 8]

Figure 7: Experienced any economic crime within the last 12 months

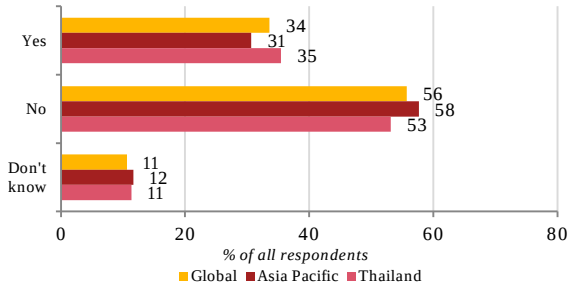
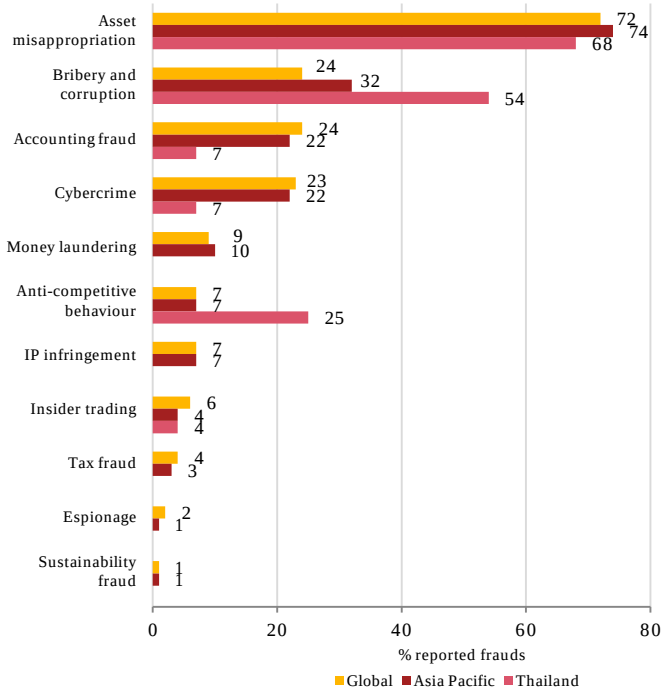


Figure 8: Types of economic crime reported



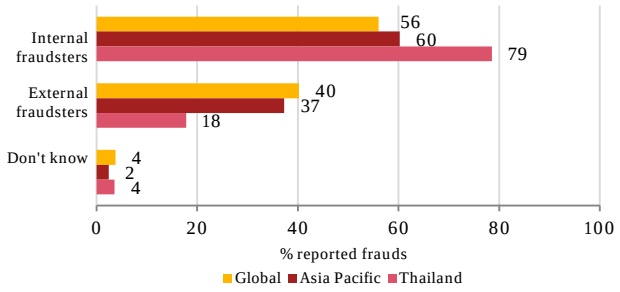
% respondents who experienced economic crime in the last 12 month

Most common sources of crime

We observed that economic crime by external fraudsters affected ***18%*** of respondents in Thailand, significantly below the Asia-Pacific and global averages of ***37%*** and ***40%*** respectively. Thai respondents reported that ***79%*** of the perpetrators are internal. [See figure 9]

Interestingly, ***11%*** of respondents did not know if their organisation had suffered fraud in the past 12 months.

Figure 9: Experience of economic crime

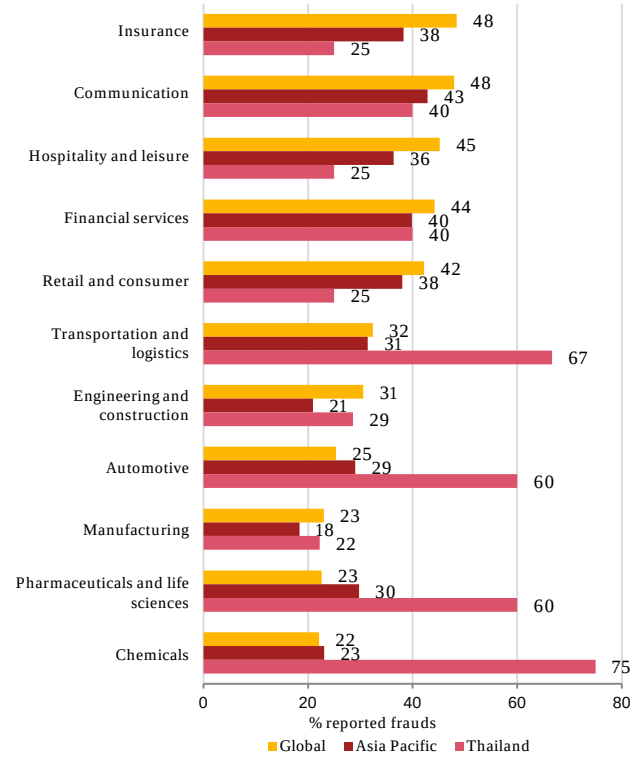


% respondents who experienced economic crime in the last 12 month

Is any particular sector experiencing high levels of fraud?

Respondents from Thailand with experience of economic crime included sectors as diverse as automotive, chemicals, engineering, financial services, manufacturing and pharmaceuticals. [See figure 10]

Figure 10: Fraud per industry sector



% respondents who experienced economic crime in the last 12 months

*Thai respondents reported that **79%** of the perpetrators are internal.*

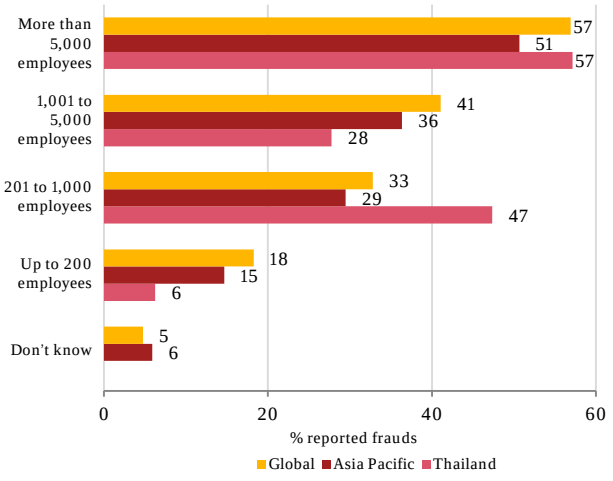
Which organisations are experiencing fraud?

Out of our survey respondents who suffered fraud, ***79%*** stated that they have been the victims of between one and 10 instances of economic crime in the past 12 months while ***18%*** were impacted by between 11 and 100 incidents.

There is an important correlation between the size of the organisation (as measured by the number of employees) and the number of fraud incidents reported. However, Figure 11 suggests that not only large companies (more than 1,000 employees) are experiencing economic crime; fraudsters are also targeting small-and-medium sized organisations. [See figure 11]

While the type of economic crime differs, fraudsters not to distinguish between the types of organisation they target: ***43%*** of targeted organisations were from the private sector and ***57%*** were listed on a stock exchange.

Figure 11: Number of employees in Thailand of the companies reporting fraud



% respondents representing different sizes of organisation

Types of economic crime

Economic crime can take on many different forms, with some being more common and persistent than others. You can earlier find from figure 8 for the top economic crimes experienced by respondents who reported being victims over the past 12 months.

Our survey previously shows that the three most common types of economic crime experienced in Thailand during the past 12 months were asset misappropriation; bribery and corruption; and anti-competitive behaviour [See figure 8]. When comparing the Thailand results to the global results of the 2011 survey, asset misappropriation ***(68%)*** is similar to global results while the responses on bribery and corruption ***(54%)*** were much higher than reported globally ***(24%)***. Interestingly, the 2011 global survey results show that there is a 'new kid on the block': cybercrime, with degree of threat similar to accounting fraud and particularly common among Thai respondents from the financial services sector. A closer look at the top three types of economic crime in Thailand over the last 12 months compared with the Asia-Pacific reveals a consistent trend in asset misappropriation, but the number of incidents of bribery and corruption and anti-competitive behaviour cases is significantly higher in Thailand than in other parts of the region.

This year's Thailand survey revealed that accounting fraud has only been experienced by ***7%*** of respondents compared to the overall global trend of ***24%***. There could be various reasons for this change but some factors that we think could have had an impact are:

1. Organisations may have instituted tighter controls.

2. Senior managers may not feel the same pressure to produce and sustain revenue growth despite the melt-down in global economy in 2009. It is also possible that the high number of fraud cases in the past couple of years dissuaded senior managers from taking risks or engaging in accounting fraud.

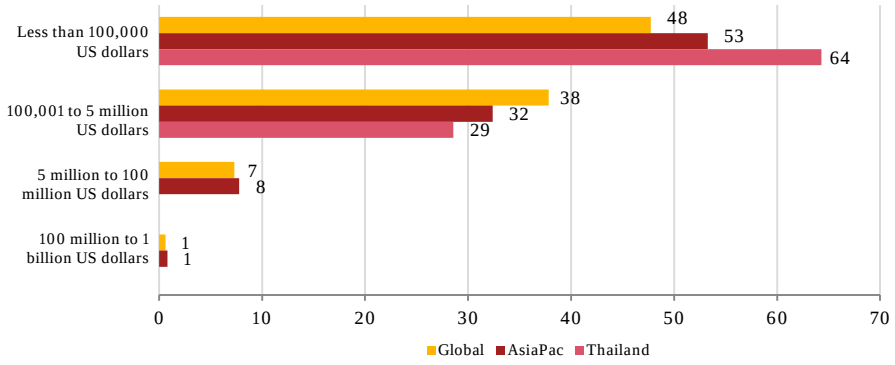
3. Lack of detection could also explain the drop in reported accounting fraud cases in Thailand. Indeed, layoffs since the economic downturn have reduced resources available for detecting and preventing accounting fraud. This means fewer internal auditors to investigate and identify fraud. It is also possible that respondents who used to classify accounting fraud involving computers, electronic devices, systems, and internet have reclassified it as cybercrime this year. As we highlighted in the cybercrime section, cybercrime can be an ambiguous term and people have varying views about what it constitutes.

More than half of economic crime cases in Thailand involved both asset misappropriation and bribery; and corruption. A closer look at the underlying data tells us that respondents from the automotive sector were most heavily affected by asset misappropriation ***(21%)*** while financial services was the sector mostly impacted by bribery and corruption ***(20%)***.

Costs of fraud

It is very difficult to gauge the financial impact of economic crime in Thailand. However, we asked our respondents to estimate, to the best extent possible, the cost of fraud. Of the Thai respondents that reported economic crime in the past 12 months, ***64%*** reported losses of up to USD100,000 and ***29%*** between USD100,000 and USD5 million. Victims of bribery and corruption reported higher costs and almost one-third lost between USD100,000 and USD5 million. [See figure 12]

Figure 12: Cost of fraud

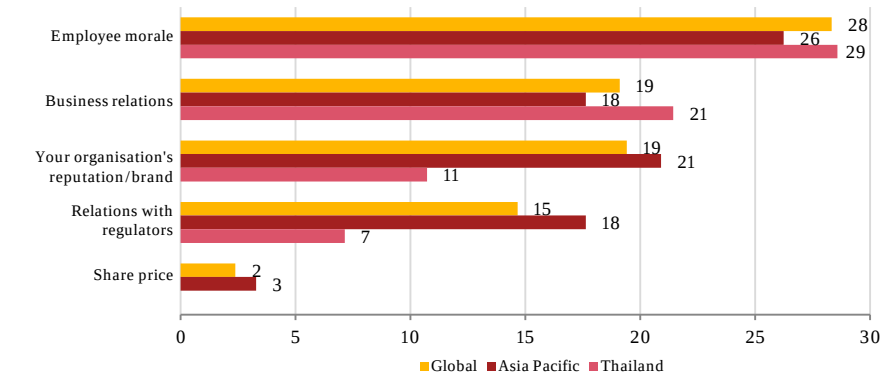


82%

Of respondents identified their own management as the main internal perpetrator

Our survey investigated both the direct losses and collateral damage suffered by organisations; including the impact of economic crime on their reputation, brand, share price, employee morale, business relations and relations with regulators. Though difficult to gauge, among those in Thailand who reported economic crime, ***29%*** saw fraud as having a significant impact on employee morale, ***11%*** on said it hurt the organisation's brand and reputation; and another ***21%*** believed that it significantly affected business relationships. [See figure 13].

Figure 13: Collateral damage



Who is committing the fraud?

Combating economic crime requires gathering as much information as possible about the perpetrators and being proactive in the fight against attacks. Identifying perpetrators and knowing where they come from can pinpoint weaknesses in an organisation's response mechanisms and internal controls. We have asked those respondents who reported economic crime to profile the perpetrators of the most serious fraud suffered by their organisation in the past 12 months.

The survey found that ***79%*** of economic crime was perpetrated by employees, with ***18%*** reporting fraud by external parties. Thailand's employee-committed economic crime results are far greater than the Asia-Pacific and Global response rates of ***60%*** and ***52%*** respectively.

With ***79%*** of the reported economic crime occurrences perpetrated internally, by individuals who may be aware of the companies' IT and internal controls, this trend emphasises the need for a robust and tailored fraud risk management framework.

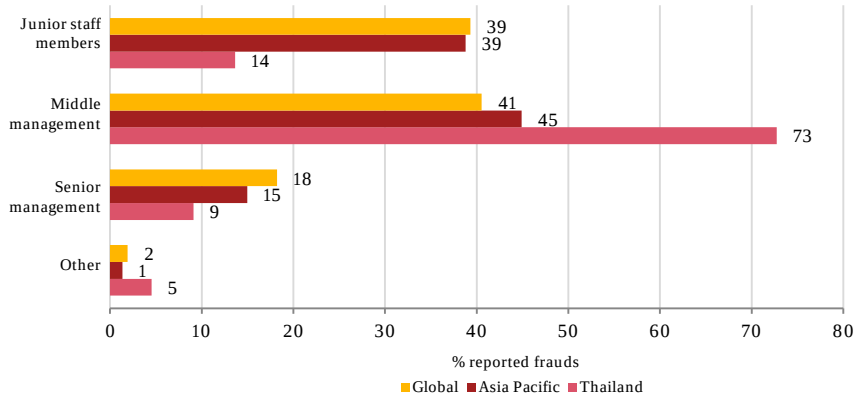
The profile of an internal fraudster

We asked our respondents to classify fraud cases committed by the organisations' own employees versus external parties. Further we divided the organisations' people into senior, middle and non-management. The survey found that ***82%*** of respondents identified their own management as the main internal perpetrator of economic crime against their organisations. Given the increasing prevalence of internal fraudsters, there is a need for organisations to improve internal controls and demonstrate a heightened awareness around fraudster profiles. [See figure 14]

This section of the report details the most frequent answers by our survey respondents. Although an economic crime can be committed by anyone, it is important to create a profile of a typical fraudster.

Our Thai respondents stated that ***82%*** of economic crime has been perpetrated by senior and middle management. This is especially concerning as economic crime committed by managers is less likely to be detected and often has a more serious impact.

Figure 14: Profile of internal fraudsters



% respondents who reported that an internal employee was the main perpetrator of fraud

Who is committing the fraud?

The profile of an external fraudster

Respondents from Thailand revealed that the first group of their external fraudsters are Agents or Intermediaries ***(60%)*** while the rest are their customers. None of them mentioned about their vendors or other types. The result from Thai companies are quite different from global and Asia Pacific regions. [See figure 15].

According to global result, the most common economic crimes perpetrated by a third or unknown party were cybercrime, asset misappropriation, bribery and corruption; and anti-competitive behaviour. Cybercrime is often perpetrated by ingenious organised criminals who are capable of protecting their identities through the internet. It is therefore no surprise that victim organisations often do not know the perpetrators' identities. However, asset misappropriation, bribery and corruption were also committed by a significant number of external fraudsters unknown to the organisations, which suggests that detection controls are insufficient when dealing with external perpetrators.

According to global result, it further demonstrates that, among the top four economic crimes, cybercrime is the only type more often committed by external fraudsters. On the other hand, three of the top four crimes, asset misappropriation, accounting fraud, and bribery and corruption, are more often committed by internal perpetrators.

What actions do organisations take against fraudsters?

Setting the right "tone from the top" to deter economic crime not only minimises the negative effects of fraud, it can also deter perpetrators and potential perpetrators.

More importantly, how a Thai company responds to economic crime will affect its standing in the eyes of its stakeholders such as investors, banks, employees and regulators. That's why it is critical to send the right signals to potential perpetrators and to carefully consider the implications, costs and benefits of all possible alternatives when dealing with economic crime. A company that is not seen to take appropriate remedial action against economic crime and misconduct might be setting an inappropriate 'tone from the top'. Employees may therefore view economic crime as acceptable, even if it is detected.

Those responsible for fraud response must consider how any investigation or decision process will be perceived by the alleged perpetrator and by others in the company. It will affect an organisation's ethical standing, the perception of its stance against fraud and its reputation for respectful treatment of employees. Hopefully, this will help Thai companies focus on improving incident response and remediation procedures once fraud is uncovered.

The Thai Survey respondents were asked what actions, if any, their organisations took against the main internal perpetrators. The most frequent response was dismissal ***(86%)***. Civil action and a warning/reprimand were given in ***23%*** of cases, and law enforcement agencies were informed in 18% of cases.

Respondents in other Asia-Pacific countries indicated that they took a less active response to fraud cases involving internal perpetrators, with fewer dismissals ***(77%)***. However, fraud cases reported to law enforcement agencies were significantly higher in other Asia-Pacific countries. [See figure 16]

It is worrying to see that, in Thailand, the 'hard-line' approach of informing law enforcement ***(18%)*** and taking civil action ***(23%)*** is relatively low compared with Asia-Pacific survey responses of ***41%*** and ***29%*** respectively. This data suggests that there is a level of complacency, or punitive action taken against fraudsters. It also suggests that fraudsters may still remain within an organisation or are gently dismissed and able to commit further crimes elsewhere.

A lack of economic crime prevention controls makes it difficult for organisations to investigate fraud and establish responsibility. Further, when investigations are performed by inexperienced personnel; or if they are not conducted at all, vital evidence often remains undiscovered. It may be unknowingly destroyed or rendered irretrievable. This is often the case where specialised e-discovery technology is used by inexperienced staff.

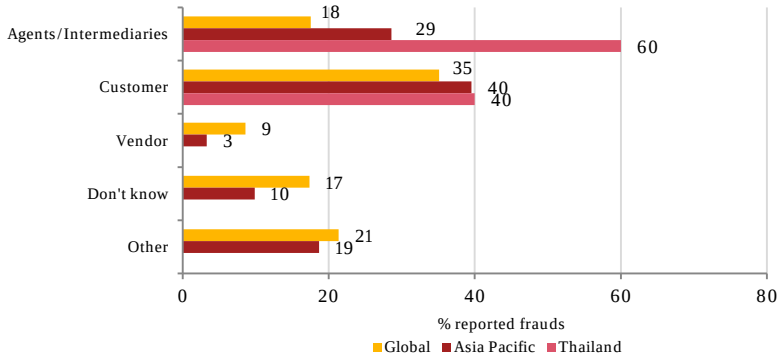
It is important for organisations to demonstrate a 'zero tolerance' policy for fraud and in order to set the right tone and convey a strong message within organisations, they should deal with the fraudster in an official and external way, rather than taking a 'soft approach' and dealing with it quietly and internally.

Organisations have a variety of tools at their disposal when dealing with external perpetrators. The majority of organisations decided to inform law enforcement bodies ***(100%)*** while ***80%*** opted for cessation of the business relationship, followed by civil action ***(60%)*** and notifying relevant regulatory authorities ***(20%)***. The lack of reporting to regulatory authorities is a matter for concern and indicates a potential lack of familiarity with reporting procedures or a low level of confidence in the regulators. It is important for Thai companies to respond to economic crime consistently. Economic crime response strategies and plans should ensure that cessation of business relationships, performance of recovery action and reporting to regulatory authorities should be based on policy rather than discretion. [See figure 17]

Effective economic crime incident response protocols will ensure that a response is made in terms of when, how, where and why the infraction occurred. It also sets specific terms of reference for investigators, and outlines reporting channels. Further responsibility for the decisions concerning sanctions should also be identified.

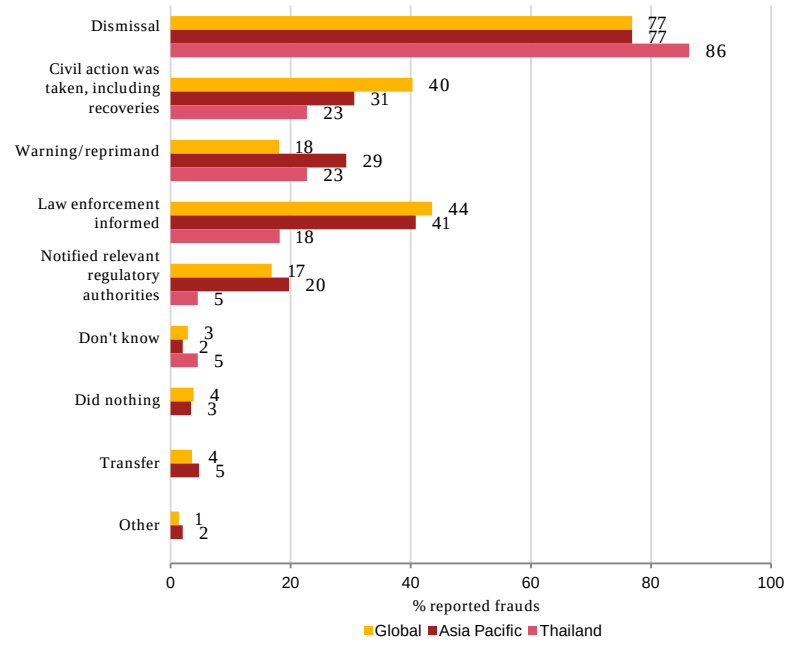
A good pre-planned economic crime incident response policy enables a Thai company to act speedily and effectively to mitigate any losses incurred through fraud. It also enables the control of potential consequences such as the loss of shareholder confidence, harm to company reputation, and regulatory enforcement. More importantly, an appropriate response helps to maintain the morale and respect of employees.

Figure 15: Profile of external fraudsters



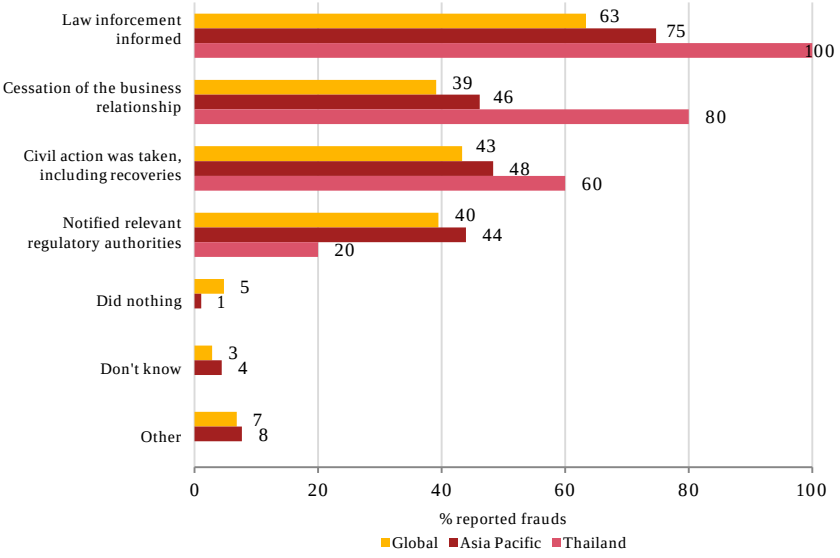
% respondents who reported that an internal employee was the main perpetrator of fraud

Figure 16: Actions against internal perpetrator



% respondents who experienced economic crime in the last 12 months

Figure 17: Actions against external perpetrators



% respondents who experienced economic crime in the last 12 months

Fraud detection

Fraud detection measures enable Thai companies to respond rapidly to threats of economic crime. This helps to prevent economic crime and minimise exposure.

Fraud detection refers to all the methods employed by organisations to identify economic crime. Such methods may include:

- Internal audits, fraud risk management, electronic and automated suspicious transaction reporting, corporate security or change of personnel/duties;
- Internal tip-off mechanisms, external tip-off lines or whistle-blowing systems; or
- External forces such as law enforcement, investigative agencies, media or others.

Understanding how economic crime is detected is critical to all Thai companies in their development of effective fraud risk management systems. The leading methods by which our Thai survey detected economic crime was through internal tip-off ***(21%)***, by accident ***(21%)*** and through internal audit ***(18%)***. The means of detecting fraud in Thailand were found to be consistent with other Asia-Pacific countries, which help to confirm the importance of detection methods in fraud management programmes.

International experience consistently shows that providing anonymous hotlines to facilitate fraud tip-offs is a simple measure to help increase the number of cases detected and to limit the size of financial losses from each case. It also serves as a deterrent to potential perpetrators.

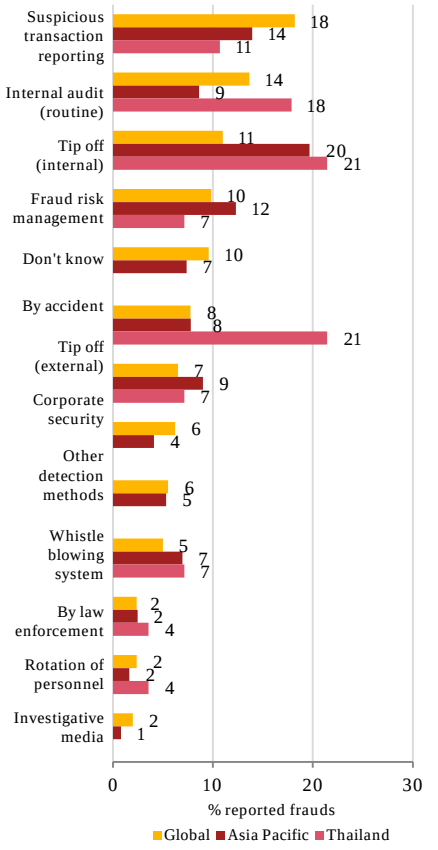
The effectiveness of internal audit to detect fraud is also important, accounting for ***18%*** of detected fraud. Internal Audit is a key component to a company's anti-fraud framework relating to the prevention and detection of fraud.

Likewise, the implementation of fraud risk management is also useful for detecting fraud ***(7%)***, as management plays a key role in the evaluation of the design and testing of the operating effectiveness of anti-fraud controls. [See figure 18]

Surprisingly, electronic and automated suspicious transaction reporting was not as effectively used in Thailand, and only ***11%*** of respondents stated that it was employed by their organisation. Economic crime needs to be tackled in a comprehensive manner and even if prevention measures are bypassed and fraud is committed, it is essential to have retrospective automated suspicious transaction reporting in place to help detect these violations and monitor for further incidents.

Electronic and automated suspicious transaction reporting is normally used to detect, investigate and fight economic crime in the financial services sector. This involves highly sophisticated tools to identify triggers and enable the organisation to investigate suspicious transactions. This detection method is based on an electronic automated system without human intervention.

Figure 18: Detection methods



% respondents who experiences economic crime in the last 12 months

Fraud risk assessments – a useful tool for detecting fraud

Thai companies trading internationally constantly have to deal with regulatory and compliance challenges in today's business environment. Changing market expectations as a result of corporate scandals are also influencing the manner in which a Thai company manages risk. How a Thai company responds and deals with fraud shapes its ethical culture. Equally important are the measures it puts in place to address the risks of economic crime and misconduct.

Fraud risk exposure can differ between organisations. An appropriately considered and tailored framework should provide the antifraud initiatives needed to manage the risks of economic crime in a manner consistent with regulatory requirements.

In order to prevent fraud, it is important for organisations to assess the risks and identify the gaps. Regular fraud risk assessments help organisations analyse their fraud exposure. Figure 19 shows the correlation between the frequency of organisations performing fraud risk assessments and the incidents reported fraud.

The global and Asia Pacific figure demonstrates that frequent fraud risk assessments increase the likelihood that fraud is detected.

Organisations that do not carry out fraud risk assessments record significantly lower numbers of total fraud events, and organisations that stated they conducted assessments once or more often reported higher numbers of fraud incidents. These figures, then, confirm the dictum of 'seek and you shall find'.

The results from Thai respondents were different from other jurisdictions with ***44%*** of Thai firms that did not perform fraud risk assessments still reporting fraud. This indicates lax fraud risk management in Thailand, where most of the frauds were reported "by accident" (see figure 18). The fact that a high percentage of fraud was reported in companies with no fraud risk assessment raises the possibility that other frauds are occurring in the companies but are going undetected.

The survey found that ***51%*** of all Thailand respondents either do not perform fraud risk assessments or do not know if they do. Of those Thai respondents who stated that they do not perform fraud risk assessments, ***34%*** said they were not sure of what it involves. Evidently, the Thai corporations are in need of greater awareness of fraud risk mitigation strategies and governance.

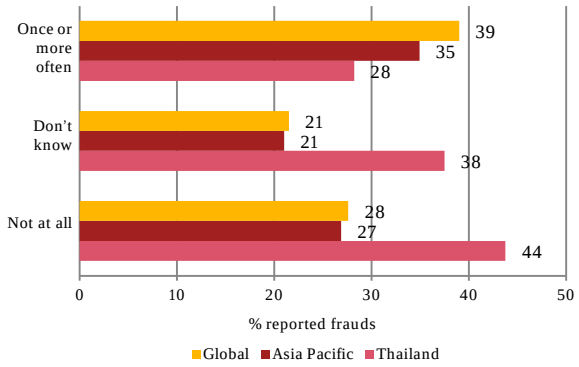
Of the Thai respondents who reported economic crime, ***28%*** had not performed a fraud risk assessment because they did not believe it was worthwhile. ***34%*** did not know whether their companies had performed assessments. [See figure 20]

Our study found that identifying and understanding fraud risks are pre-conditions to instituting detective anti-fraud measures. Without this approach, only the most obvious fraud risks are assessed for their impact and significance. Unfortunately, fraud is usually simple in nature and employees have the opportunity and time to learn weaknesses and exploit them.

This appears to be an educational and awareness issue and work needs to be done regarding the value, effectiveness, quality and necessity of performing regular fraud risk assessments. In addition, awareness needs to be raised that fraud risk assessments are a valuable tool in detecting fraud and in the fight against it.

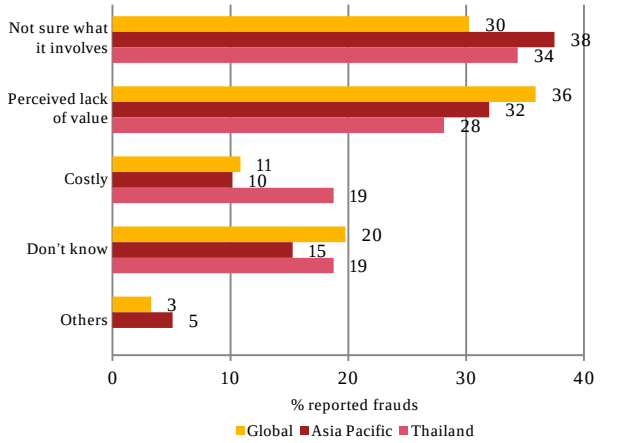
Companies should ensure that employees are aware of the risks of economic crime and are alert to 'red flags'. Understanding anti-fraud measures is essential to the success of a company's fight against fraud.

Figure 19: Percentage of reported frauds in the last 12 months in relation to the frequency of fraud risk assessments



% respondents who experienced economic crime in the last 12 months

Figure 20: Reasons for not performing fraud risk assessments



Conclusion

New ways of doing business, new technologies and changing work environments bring new risks and new ways for fraudsters to commit crime. Organisations need to be aware of these changes and adapt their response mechanisms and detection methods. Survey results from Thai corporations drew similar conclusions to those of the global survey; namely that fraud is persistent and that organisations need to be much more proactive in fighting economic crime.

'Traditional' frauds in Thailand like asset misappropriation, accounting fraud, anti-competitive behaviour and bribery and corruption remain the top problems reported by Thai respondents over the past 12 months. But 'new' types of fraud are emerging globally – cybercrime in particular - although it is not yet recognised as a prevalent threat in Thailand. This is even more true when it comes to new technology. Smart phones, tablet devices and cloud computing can offer a wealth of attractive business solutions and opportunities, but they can also be a Pandora's box of risks and dangers. Having a smart phone or a tablet device means carrying around your organisation's central server in your pocket – without precautions in place, anyone might be able to access sensitive and confidential information and cause considerable harm, both financial and collateral.

A decade on and the fraud risk continues to rise. Although your firm might already have effective risk management systems, there are always individuals or groups who are able to spot an opportunity and circumvent or override controls. This is especially true when it comes to cyber security. As headcounts fall in control functions across the globe, we fear more fraud will go undetected.

Advances in technology are fast paced and fraudsters are usually not far behind. But organisations often are. It is now essential to ensure that cyber and information security issues have the standing they warrant on an organisation's risk register. Those organisations ready to understand and embrace the risks and opportunities of the cyber world will be the ones to gain competitive advantage in today's technology-driven environment.

Organisations in Thailand in particular should also ensure that they have a comprehensive understanding of their own fraud risks and figure out the right mitigation approaches. Establishing the right "tone at the top" and a channel for whistleblowers are also the key in the fight against economic crime.

Methodology and acknowledgments

Our sixth Economic Crime Survey was conducted globally, including Thailand, between July and November 2011. The survey comprised three sections: (1) general profiling questions; (2) comparative questions centring on the experience of economic crime; and (3) cybercrime as this survey's focus topic. Overall, 3,877 respondents from 72 countries, including 79 from Thailand, participated in the survey by filling in an online questionnaire. The participants were asked to respond to the questions with regard to (a) their organisation, and (b) the country in which they are mainly based.

The 2011 survey was based on the following research strategies:

1. Survey of organisation executives: The survey findings derive from executives' reports of their experiences and perceptions of economic crimes in their organisations. We surveyed the respondents to obtain information on: (i) the different types of economic crime; (ii) their impact on the organisation in regard to both financial and collateral damage; (iii) the perpetrators of these crimes; as well as (iv) the remedial action taken and the crime response mechanisms in place.

2. Questions relating to cybercrime: Our survey offers in-depth insights into the increasing significance of cybercrime and corporate vulnerability to such attacks. Our focus on this economic crime type has allowed us to understand the impact of cybercrime at the corporate level and reflects the growing importance of the internet.

Asia Pacific	796
Australia	79
Hong Kong (and China)	22
India	106
Indonesia	84
Japan	73
Malaysia	93
Middle Eastern Countries*	127
New Zealand	93
Papua New Guinea**	1
Singapore	18
Taiwan**	2
Thailand	79
Vietnam	19

South and Central America	483
Argentina	77
Bolivia**	3
Brazil	115
Chile**	1
Colombia**	1
Ecuador	11
Mexico	174
Peru	17
Venezuela	84

Western Europe	1,317
Andorra**	1
Austria**	8
Belgium	84
Cyprus**	5
Denmark	116
Finland	61
France	112
Germany	38
Greece	92
Ireland	80
Italy	127
Luxembourg**	3
Netherlands	41
Norway	67
Spain	85
Sweden	79
Switzerland	140
UK	178

North America	209
Canada	53
USA	156

Central and Eastern Europe	804
Bulgaria	58
Croatia**	1
Czech Republic	84
Estonia**	1
Hungary	85
Lithuania**	7
Moldavia**	1
Montenegro**	1
Poland	79
Romania	76
Russia	126
Serbia	14
Slovakia	84
Slovenia	48
Turkey	55
Ukraine	84

Africa	260
Angola**	1
Botswana**	1
Ghana	29
Kenya	91
Liberia**	5
Namibia**	2
Nigeria**	3
South Africa	123
Sudan**	1
Swaziland**	1
Tunisia**	2
Zambia**	1

No primary country specified	8

TOTAL	3,877

** Middle East countries include participants from Middle East and Israel.*

*** These are individual participants who found our survey and participated online.*

Table 2: Participating industry group

	% organisations
Aerospace and defence	0.60%
Automotive	3.90%
Chemicals	2.20%
Communication	3.10%
Education	1.10%
Energy, utilities and mining	7.00%
Engineering and construction	5.20%
Entertainment and media	2.80%
Financial services	17.70%
Food-related	1.40%
Government/state-owned enterprises	4.70%
Health and care	0.90%
Hospitality and leisure	1.90%
Insurance	4.90%
Manufacturing	11.60%
Pharmaceuticals and life sciences	4.60%
Professional services	6.20%
Property	1.50%
Retail and consumer	8.40%
Technology	4.60%
Transportation and logistics	4.40%
Other industries/business	1.10%

Table 3: Organisation types participating

	% organisations
Private	51.40%
Listed on a stock exchange	36.10%
Government/state-owned enterprises	10%
Cooperative/non-profit	2.50%

Table 4: Size of participating organisations

	% organisations
Up to 200 employees	31.60%
201 to 1,000 employees	29.40%
1,001 to 5,000 employees	21.70%
More than 5,000 employees	16.20%
Don't know	1.10%

Table 5: Function (main responsibility) of participants in the organisation

	% organisations
Finance	29.20%
Executive management	17.40%
Audit	15.90%
Risk management	5.70%
Compliance	5.30%
Security	3.90%
Legal	3.80%
Information technology	3.60%
Advisory/Consultancy	3.30%
Operations and production	2.60%
Marketing and sales	2.40%
Human resources	1.40%
Tax	1.20%
Customer service	1.00%
Research and Development	0.70%
Procurement	0.40%
Other	2.20%

Table 4: Job title of participants in the organisation

	% organisations
Chief Financial Officer / Treasurer / Comptroller	23.40%
Manager	17.40%
Head of Department	14.80%
Other C-level Executive	10.40%
Chief Executive Officer / President / Managing Director	10.20%
Senior Vice-President / Vice-President / Director	7.60%
Head of Business Unit	7.10%
Board member	3.90%
Chief Information Officer / Technology Director / Chief Security Officer	2.70%
Chief Operating Officer	2.30%
Others	0.20%

SIDBA
SIDBA

Terminology

Due to the diverse descriptions of individual types of economic crime in countries' legal statutes, we developed the following categories for the purpose of this survey. These descriptions were defined in the web survey to assist respondents.

Economic crime or fraud
The intentional use of deceit to deprive another of money, property or a legal right.

Asset misappropriation (including embezzlement/deception by employees)
The theft of assets (including monetary assets/cash or supplies and equipment) by directors, others in fiduciary positions or an employee for their own benefit.

Accounting fraud
Financial statements and/or other documents are altered or presented in such a way that they do not reflect the true value or financial activities of the organisation. This can involve accounting manipulations, fraudulent borrowing/raising of finance, fraudulent application for credit and unauthorised transactions/rogue trading.

Corruption and bribery (including racketeering and extortion)
The unlawful use of an official position to gain an advantage in contravention of duty. This can involve the promise of an economic benefit or other favour, the use of intimidation, or blackmail. It can also refer to the acceptance of such inducements.

Money laundering
Actions intended to legitimise the proceeds of crime by disguising their true origin.

IP infringement (including trademarks, patents, counterfeit products and services)
This includes the illegal copying and/or distribution of fake goods in breach of patent or copyright, and the creation of false currency notes and coins with the intention of passing them off as genuine.

Insider trading
Insider trading refers generally to buying or selling a security in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non-public information about the security. Insider trading violations may also include 'tipping' such information, securities trading by the person 'tipped', and securities trading by those who misappropriate such information.

Espionage
Espionage is the act or practice of spying or of using spies to obtain secret information or using technology to act on your behalf as spies.

Financial performance
This can be defined as measuring the results of an organisation's policies and operations in monetary terms. These results are reflected in return on investment, return on assets and value added; typically, in the private sector, returns will be measured in terms of revenue; in the government/state-owned enterprises, returns will be measured in terms of service delivery.

Fraud risk assessment
Fraud risk assessments are used to ascertain whether an organisation has undertaken an exercise to specifically consider:

1. The fraud risks to which operations are exposed;
2. An assessment of the most threatening risks (i.e., evaluation of risks for significance and likelihood of occurrence);
3. Identification and evaluation of the controls (if any) that are in place to mitigate the key risks;
4. Assessment of the general anti-fraud programmes and controls in an organisation; and
5. Actions to remedy any gaps in the controls.

Fraud triangle
The 'fraud triangle' describes the interconnected conditions that act as harbingers to fraud: opportunities to commit fraud, incentives (or pressure) to commit fraud, and the ability of the perpetrator to rationalise the act.

Senior executive
The senior executive (for example the CEO, Managing Director or Executive Director) is the main decision-maker in the organisation.

Cybercrime
Also known as computer crime, cybercrime is an economic offence committed using the computer and the internet. Typical instances of cybercrime are: the distribution of viruses; illegal downloads of media; phishing and pharming; and theft of personal information, such as bank account details. This excludes routine fraud whereby a computer has been used incidentally to create the fraud and only includes such economic crimes where computer, internet or use of electronic media and devices is the main element and not an incidental one.

Sustainability activities
Includes activities such as carbon credit trading (buying and selling carbon credits), in projects which create carbon emissions offsets.

Sustainability fraud
Fraud in relation to sustainability activities (refer to 'Sustainability activities' above), such as carbon trading markets, environmental claims or statutory declarations.

Anti-competitive behaviour
Includes practices that prevent or reduce competition in a market, such as cartel behaviour involving collusion with competitors (for example, price fixing, bid rigging or market sharing) and abusing a dominant position.

Financial losses
When estimating financial losses due to fraud, the participants should include both direct and indirect loss. The direct losses are the actual amount of fraud and the indirect losses would typically include the costs involved in investigating and remedying the problem; penalties levied by the regulatory authorities, litigation costs, and reputational damage. This should exclude any amount estimated due to 'loss of business opportunity'.

Cybercrime incident response mechanism
This would typically include in-house technical capabilities to prevent, detect and investigate cybercrime, access to forensic technology investigators, media and PR management plans; controlled emergency network shutdown procedures, etc..

About PwC Forensic Services
The Forensic Services Group of PwC's global network of firms plays a lead role in addressing the life cycle of fraud and other avoidable losses, providing reactive investigative services and proactive remedial and compliance to clients in the public and private sector.

Contacts

Vorapong Sutanont
Partner
Forensic Services
PricewaterhouseCoopers FAS Ltd.
Tel: +66 (0) 2344 1429
Fax: +66 (0) 286 4440
vorapong.sutanont@th.pwc.com

www.pwc.com/th