# *Economic crime remains an obstinate threat in Singapore*

## Preparedness to keep pace with evolving challenges is crucial

**22%**

More than 1 in 5 organisations in Singapore report being victims of economic crime

**43%**

Cybercrime jumped from 15% in 2014; now the second most prevalent economic crime in Singapore

**45%**

In anti-money laundering areas, complexity of implementing and upgrading transactions monitoring systems was the most significant challenge faced by financial institutions

pwc

*www.pwc.com/sg/crimesurvey*

# Contents

*Although Singapore-based companies are reporting lower incidences of fraud compared to the global average, emerging new threats require companies to adjust their line of defence.*

# *Foreword*

In today's business landscape, companies are constantly facing the delicate task of balancing risks, costs and opportunities, more so with the recent global economic slowdown.

Intense efforts by companies and authorities to strengthen measures to prevent, detect and combat fraud are matched with heightened regulatory standards in Singapore. This favourable environment certainly helped to maintain the positioning of Singapore as a safe business place which continued to experience a lower rate of economic crime compared to both Global and Asia Pacific.

This business friendly environment contributes to the success of local businesses and also attracts foreign companies to establish a presence in Singapore. However, companies should continue to be vigilant, as businesses are increasingly integrated in global and regional economies.

As the threats and risks of economic crime are greater in the higher risk territories outside of Singapore, controls and processes producing positive results in Singapore may be less effective in higher risk territories. In addition, unlike the high level of confidence Singapore companies have in our local law enforcement agencies, such reliance may be of much lower levels in other territories.

Understanding these challenges and knowing what appropriate actions to take are crucial for companies to navigate the murky waters of age-old problems of bribery and corruption to more modern, sophisticated cybercrime. It means that organisations should be aware of their risks and be ready to quickly mobilise internal or external specialists when the need arises.

In general, reinforcement of corporate controls has proven its effectiveness in fraud detection – from suspicious transaction reporting to fraud risk assessments. It is no surprise that more companies see the value in these measures and go the extra mile to strengthen their line of defence against fraud. An effective compliance programme does not end with its implementation but requires continuous monitoring, updating and fine-tuning to stay flexible and agile in order to meet tomorrow's challenges.

We believe this report provides valuable insights for companies – to adjust the lens on economic crime and focus on making strategic preparations for future challenges and opportunities.

**Chan Kheng Tek**
PwC Singapore Forensics Leader
February 2016

Scan to view Kheng Tek's thoughts on the subject

*In the last 24 months, 22% of Singapore-based companies fell victim to economic crime*

# Economic crime remains an obstinate threat

More than one fifth of organisations based in Singapore experienced some form of economic crime in the past 24 months. The rate of economic crime reported in 2016 (22%) remains largely unchanged for the country since 2014 (24%), and has been consistently below the global average (36%).

However, within Asia Pacific, 30% of organisations reported having suffered from fraud over the last 24 months, this statistic being closer to the global average. This result is not unexpected and aligns with the perception of lower levels of corporate governance and higher risk of corruption within the region. The contrast between domestic and regional environments presents a true challenge for Singapore based companies, as their business activities are increasingly cross-border.

The Singapore government is well recognised for its zero tolerance for fraud and corruption. However despite the strong tone at the top, a robust legal framework and strict corporate governance, economic crime remains an obstinate threat in Singapore. The recent cases in Singapore are evidence that fraud can still occur in both public and private sectors.

*Effort invested by the Singapore government to strengthen resources in the Corrupt Practices Investigation Bureau (CPIB) raises confidence:*

***59% of Singapore participants (compared to 29% in Asia Pacific) believe that the local law enforcement agencies are adequately resourced and trained to investigate and prosecute economic crime.***

From the corporate perspective, it is encouraging to see that Singapore companies have not been complacent and have continued to be vigilant by strengthening measures to detect and combat fraud. Our survey showed that organisations are putting in more effort to minimise the risk of fraud by embarking on regular fraud risk assessments and implementing systems to monitor suspicious transactions.

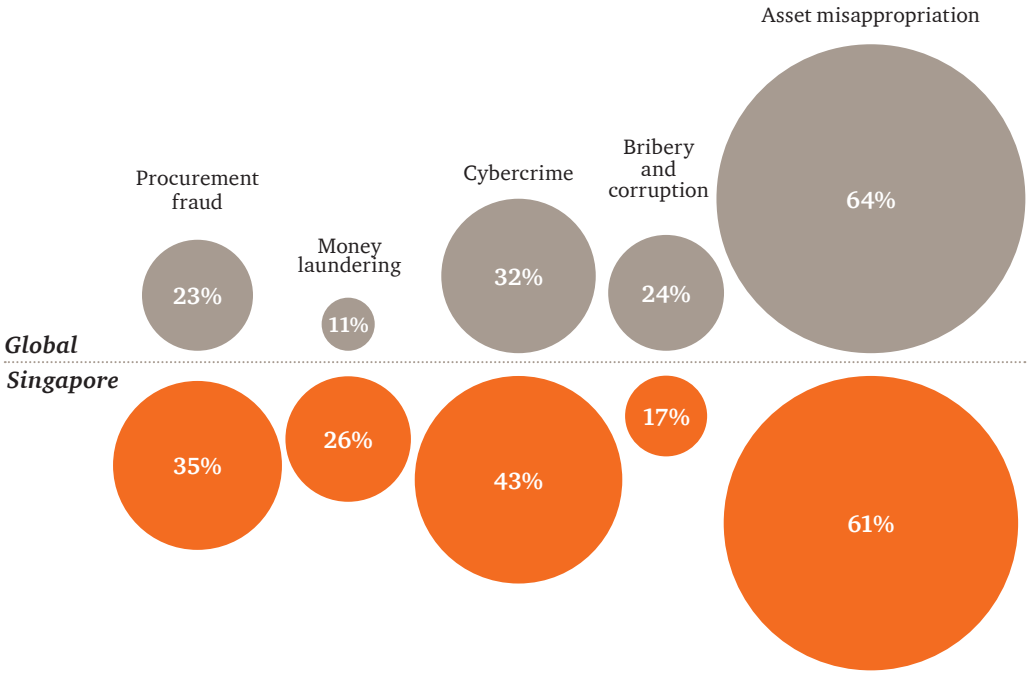
# Top 5 economic crimes in Singapore

The five most pervasive economic crimes reported in 2016's survey in Singapore are asset misappropriation (61%), cybercrime (43%), procurement fraud (35%), money laundering (26%) and bribery and corruption (17%).

Globally, asset misappropriation (64%) and cybercrime (32%) also occupy two leading positions, followed by bribery and corruption (24%), procurement fraud (23%) and accounting fraud (18%).

**Figure 1: Top 5 economic crimes in Singapore**


**Figure 2: Top 5 crimes: Singapore versus Global**




Cybercrime incidents targeting Singapore based companies have risen sharply from 15% in 2014 to 43% in 2016, becoming the second most prevalent economic crime in Singapore following asset misappropriation. This sharp rise certainly reflects the cross-border nature of cyber criminality.

These statistics are particularly alarming when we consider the threat it represents for Singapore companies, especially from a cyber security readiness perspective, and for local enforcement authorities which are often limited by national boundaries.

High rate of procurement fraud appears consistent with what we are seeing based on our experience of conducting such investigations over the past two years.

## Asset misappropriation

Asset misappropriation – theft or embezzlement of cash, inventory and company's assets by management or employees is by far the most frequently experienced type of economic crime, both in Singapore and globally. This year, the percentage of asset misappropriation incidents (61%) is at an all-time low since 2009. In fact, there has been a steep and steady decrease in the reported rates of this economic crime since 2011.

While this trend appears to be encouraging, it does not mean that fraud incidents are on the decline. Instead, it could mean that fraudsters are using more sophisticated approaches which may not be detected and prevented by existing controls in the organisations. It would be a great concern if management is unable to identify these fraudulent schemes and are therefore, unable or ill-prepared to deal with them. Therefore, under these circumstances, organisations cannot afford to be complacent but should continue to monitor and assess risks as their businesses evolve.

## Cybercrime

Singapore is becoming more of a target for cyber criminals. In this year's survey, cyber related incidents have risen sharply and are now the second most prevalent economic crime. This year, 43% of respondents that suffered an economic crime were hit by a cyber incident compared to only 15% in 2014. Consistent with this figure, the number of companies that believe they will suffer from cybercrime in the next 24 months increased to 37% (2014: 11%). This is in line with the official data published by the Singapore Police Force showing an increase by 65.6% in the number of cases related to cybercrime compared to 2014[1].

The costs resulting from cybercrime can be significant. Besides the direct cost damage, the secondary costs resulting from illicit cyber activities are also of great concern. While 13% of Singapore-based companies reported an estimated direct loss ranging from US$ 100,000 up to US$ 1 million due to cybercrime, the Monetary Authority of Singapore (MAS) estimated the overall financial damage including costs for data loss or unplanned downtime to be around S$ 1.9 billion[2] in 2014.

Despite the increased risk, less than half of the Board members request information about their organisation's state of cyber-readiness. Another concern we observed is that most companies are not adequately prepared to deal with cyber-attacks. More than half do not have an incident response plan that is fully operational.

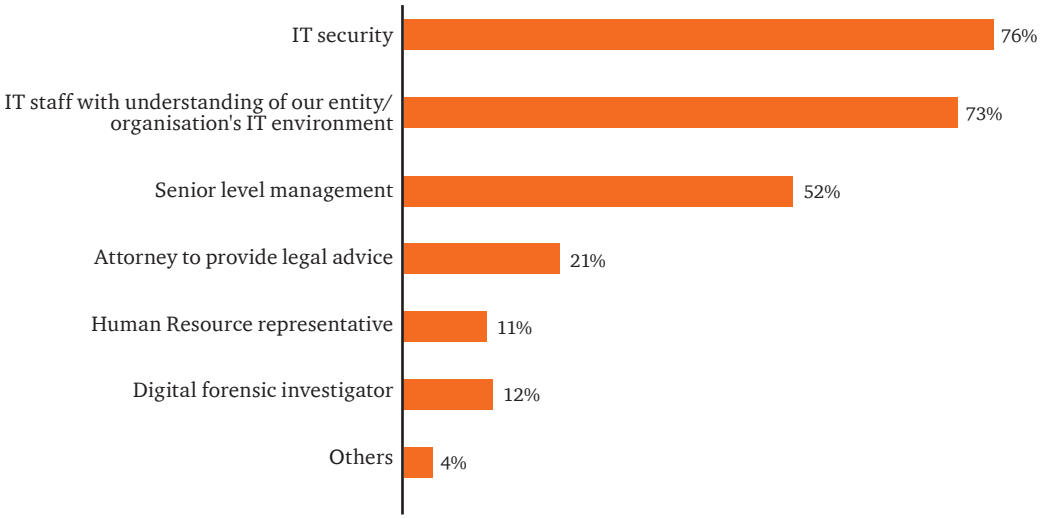
There is much catch up for these organisations. In the public sector, the Singapore government is beefing up its capabilities to fight cybercrime with an increased budget, developing a masterplan for the national Cyber Security Agency (CSA) and enhancing the Cyber Watch Centre (CWC) as well as Threat Analysis Centre (TAC). The INTERPOL Global Complex for Innovation (IGCI) has also established a presence in Singapore. This may be an excellent opportunity for organisations to capitalise on government programmes and infrastructure, e.g. by forming alliances to build competencies and sharing knowledge to tackle emerging cyber threats.

The survey revealed that 74% of participants have first responder teams to manage cyber breaches. While IT security staff are included in a significant majority of the teams, digital forensic investigators are however, only included in one in ten teams.

[1] http://www.police.gov.sg/img/stats/midyearcrimebrief2015.pdf

[2] http://www.todayonline.com/singapore/cybercrime-costs-hit-s2b-insurance-take-low

**Figure 3: Which of the following types of specialists are included in your first responder team?**




Organisations need to realise that while deploying an IT team may be an effective stop gap measure in fraud detection, a holistic responder team that includes professionals such as legal advisors and digital forensic investigators will be more beneficial in the long term.

Given the evolving nature and complexity of cyber threats, organisations cannot afford to have a myopic view of these threats where IT teams simply stay on the defensive. The various specialists within the responder team can value add in several ways. For instance, leveraging external specialists with experience in dealing with similar fraud incidents can help organisations to better assess and mitigate the impact of threats from both financial and reputational point of views.

## Procurement fraud

Based on our survey, Singapore companies experienced a higher rate of procurement fraud (35%) as compared to their Asia Pacific counterparts (27%). More than 75% of respondents who experienced a procurement fraud reported that the fraud occurred at the beginning of the procurement process (i.e. during bidding and vendor selection).

*20% of respondents believe that their organisation will be affected by a fraud incident related to procurement over the next 2 years.*

*Given the high volume of procurement transactions performed by an organisation each year, how confident are you that each of them is valid and properly authorised?*

With regional and global economies experiencing a downturn, organisations are likely to scrutinise cost centres to implement cost cutting measures. The procurement department is one of the units that typically faces such scrutiny. Organisations should be mindful that cost-cutting measures do not compromise existing controls to mitigate the risk of procurement fraud.

## Money laundering

In the last several years, the MAS has been conducting a broad range of anti-money laundering inspections among financial institutions based in Singapore. The heightened scrutiny seems to be reflected in the survey results, as 70% of the respondents reported that their organisations had been inspected or were under an enforced remediation programme.

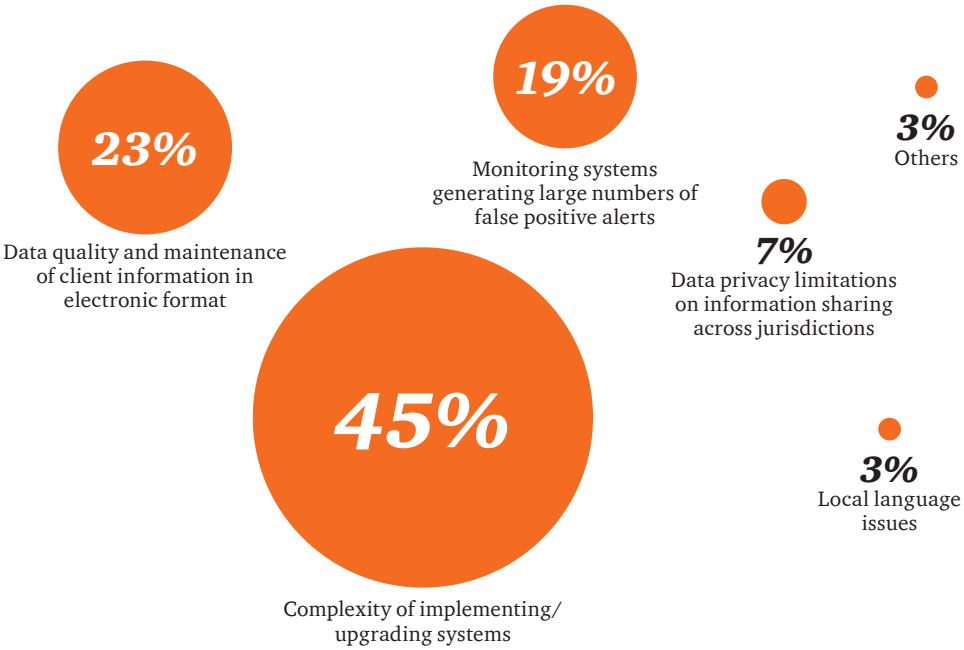
In 2015, MAS released enhanced notices and guidelines on the Anti-Money Laundering (AML) and Countering Financing of Terrorism Act (CFT), outlining increased requirements and expected standards. The regulatory landscape in Singapore is hence changing rapidly as the enhanced expectation of MAS and global best practices filter down to our local regulations. The increase in activities by regulators may have uncovered or at least triggered the discovery of AML/CFT related violations as 26% of respondents reported money laundering incidents in 2016, compared to only 5% in 2014.

On the flipside, as a result of this increased focus, 29% of the financial institutions in Singapore compared to 19% globally reported that they are struggling with the pace of regulatory changes. With regard to compliance with AML/CFT requirements, both Singapore and Global financial institutions are also facing challenges in hiring experienced AML/CFT staff, and coping with technology requirements.

In response to the increased regulatory pressure, financial institutions in Singapore have increased investments in monitoring systems, including transaction surveillance. When asked about the most significant challenge they face in relation to their AML/CFT systems, 45% of Singapore respondents compared to 24% globally stated that they are struggling with the complexity of implementing and upgrading them.

In our view, this is only a phase. Financial institutions in Singapore are currently undergoing a remediation period. The outcome of the 2015 Financial Action Task Force (FATF) evaluation on Singapore and the enhanced regulations, will strengthen Singapore's defences in fighting money laundering and countering terrorism financing.

**Figure 4: Where are you currently experiencing the most significant challenge in relation to your AML/CFT systems?**



## Bribery and corruption

At 17%, bribery and corruption remains one of the major economic crimes suffered by Singapore-based companies, although this figure is lower than the regional average of 28%. These results highlight the substantial risk that companies and businesses with footprints, or intending to expand, in other South East Asia territories may experience.

Governments around the region are stepping up enforcement and there is greater cross-border cooperation among enforcement agencies than before. Laws are also being fine-tuned to give more focus and clarity to bribery and corruption offences.

It is encouraging to see that among the Singapore respondents, action is being taken to address this risk, as a significant majority (91%) of Singapore-based companies have in place a formal business ethics and compliance programme and 95% of Singapore-based respondents have a Code of Conduct that covers this risk area.

Having a formal Code of Conduct and structured compliance programmes are essential in mitigating bribery and corruption risks. However, organisations have to be mindful to walk the talk, and ensure such policies and programmes are embedded in the organisation's DNA. Time and again, we see ineffective deployment in many organisations' compliance programmes.

**Figure 5: Why do so many compliance programmes fail?**

Common themes observed during anti-bribery/corruption reviews include:


*Having a compliance programme in place is a step in the right direction, but deploying it well and effectively maintaining it through time is equally important.*

*In this challenging business environment, how robust is your compliance programme in addressing such risks? How would your organisation fare in the face of regulatory scrutiny?*

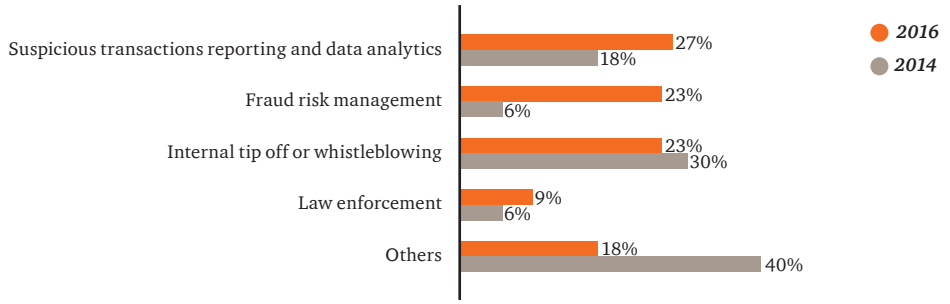
# Dealing with threats: React efficiently, prevent effectively

More than half of the respondents (55%) felt that the main contributing factor to economic crime were weaknesses in business processes which were exploited by the perpetrators. Although it is the most significant factor, this figure has decreased from 2014 (77%), aligning with the observation that more Singapore-based companies are implementing corporate control measures (i.e. fraud risk management, suspicious transactions reporting and data analytics) to detect and prevent fraud.

## Detecting fraud

The top three detection methods for organisations that experienced fraud were suspicious transactions reporting and data analytics (27%), fraud risk management (23%) and internal tip off or whistleblowing (23%).

**Figure 6: Thinking about the most serious (in terms of monetary loss) economic crime your organisation experienced in the last 24 months, how was the crime initially detected?**




Collectively these three detection methods account for 73% of total cases in 2016 as compared to 54% in 2014. This illustrates a positive trend, where companies effectively accelerate detection of frauds through activities carried out by their corporate control functions (fraud risk management, suspicious transactions reporting and data analytics) and by increasing awareness of employees (internal tip-off). Ultimately, early detection limits potential costs from fraudulent activities.

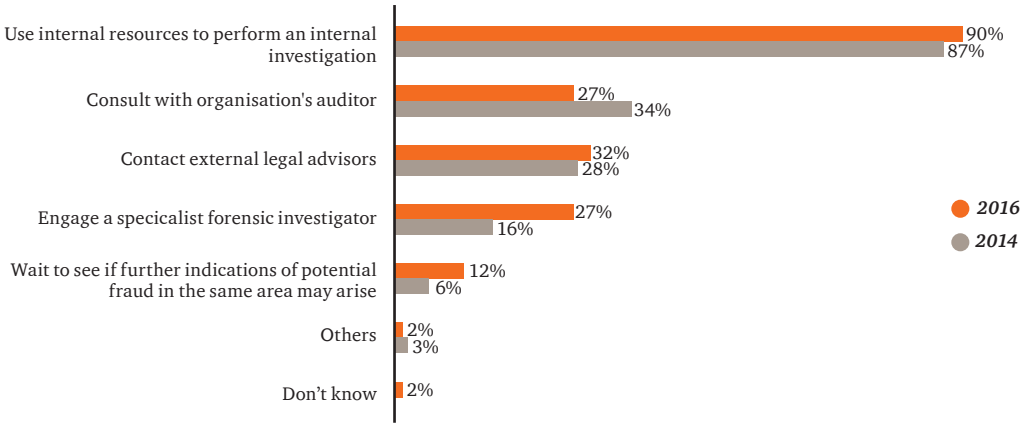
## Regular risk assessments: An essential line of defence against economic crime

To gain further insight into fraud risk management practices of Singapore-based organisations, we asked respondents about their frequency in conducting fraud risk assessments. The response was encouraging as 66% said that they conduct an assessment at least once a year, compared to 51% in 2014. However, there is still room for improvement as 30% of respondents either do not or are unaware of whether their organisations perform any fraud risk assessment, though the figure has decreased from 35% in 2014.

## Leveraging external resources for fraud investigations

Our survey also revealed that in the past 24 months, Singapore respondents (86% in 2016 compared to 78% in 2014) are increasingly receptive to engaging external parties such as legal advisors, external auditors, and specialist forensic investigators when they identify any incident of potential fraud.

**Figure 7: When your organisation identifies an incident of potential fraud, which action(s) are likely to be taken?**




In our view, this is consistent with the strong emphasis on corporate governance in Singapore businesses and suggests that more organisations are willing to take strong disciplinary measures to set the right tone (e.g. initiating legal action or seeking legal recourse, and reporting to the authorities or law enforcement agencies). This echoes the finding that Singapore respondents are confident of our local law enforcement agencies and our strong legal framework.

More organisations are also reaching out to experts and specialists to ensure investigations conducted are unbiased, thorough and conclusions sufficiently robust to withstand legal challenge.

We also observed a growing trend of organisations engaging forensic technology specialists to sieve and plough through electronic data as part of their economic crime investigations. The use of external resources in this area appears to be particularly cost-effective for many organisations that would not need this type of specialised resources and technology investments internally on a permanent basis, but only for the period of investigation.

# Contacts


**Chan Kheng Tek**
PwC Singapore
Partner, Forensics Leader
+65 6236 3628
kheng.tek.chan@sg.pwc.com

**Jimmy Sng**
PwC Singapore
Partner, Cybersecurity
+65 6236 3808
jimmy.sng@sg.pwc.com

**Dmitry Kosarev**
PwC Singapore
Director, Forensics
+65 6236 4141
dmitry.kosarev@sg.pwc.com

**Sebastian Ahrens**
PwC Singapore
Director, Forensics
Technology Services
+65 6236 3169
sebastian.ahrens@sg.pwc.com

Scan to read the full report

*www.pwc.com/sg/crimesurvey*