2020

Economic crime reported by Singapore-based companies converges towards global average

Prepare. Respond. Emerge stronger

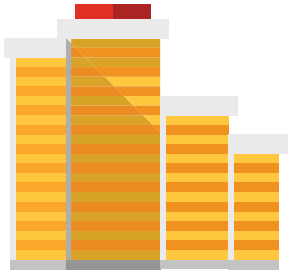
PwC's Global Economic Crime and Fraud Survey
- Singapore report

pwc

Key highlights

42%

of Singapore-based companies experienced fraud over the last 24 months



USD 50M

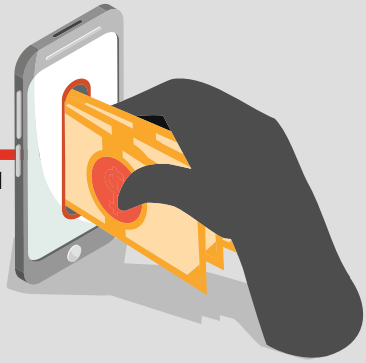
of cumulative losses reported by each of nearly a quarter of respondents

39%

of Singapore-based respondents have no formal risk assessment

51%

of frauds were committed by external perpetrators



3 out of 4 respondents

in Singapore upgraded their technology used to combat fraud

Less than 1 in 3

Singapore-based companies feel they are in a better position after experiencing and remediating a fraud

Introduction: The Singapore story

The continued rise of fraud and economic crime is impacting many more Singapore-based companies in more diverse ways. This poses some difficult questions for organisations: is our risk management programme agile enough to meet the dynamic challenges being thrown up by a globalised business environment? Are we leveraging technology effectively? How are we responding in crisis situations? Are we prepared for the worst-case scenarios?

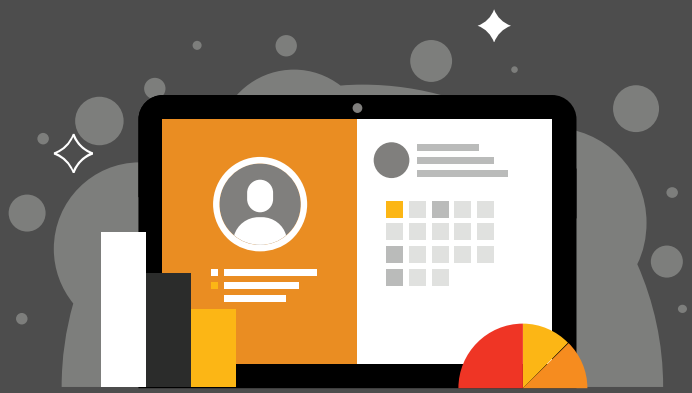
For over 20 years, PwC's Global Economic Crime and Fraud Survey has analysed fraud and economic crime worldwide to enable companies to navigate the fraud risk landscape.

With in-depth and timely insights, the survey not only identifies how and why fraud is occurring but also highlights the changing face of economic crime. Importantly, we look to understand what companies are doing to successfully mitigate such risks and challenges.

We encourage you to take this Singapore report of PwC's Global Economic Crime and Fraud Survey 2020 as a prompt for meaningful reflection. The survey results are a call to action for all local companies to prepare, respond and emerge stronger.

PwC's Global Economic Crime and Fraud Survey looks at a number of crimes, including:

1. Accounting and financial statement fraud
2. Anti-Competition and Antitrust Law Infringement
3. Asset misappropriation
4. Bribery and corruption
5. Customer fraud
6. Cybercrime
7. Deceptive business practice
8. Human Resources fraud
9. Insider and unauthorised trading
10. Intellectual Property theft
11. Money laundering and sanctions
12. Procurement fraud
13. Tax fraud



Profile of Singapore-based survey respondents

Individuals participating in the survey had job functions which give them a good understanding of various issues faced by their organisations.

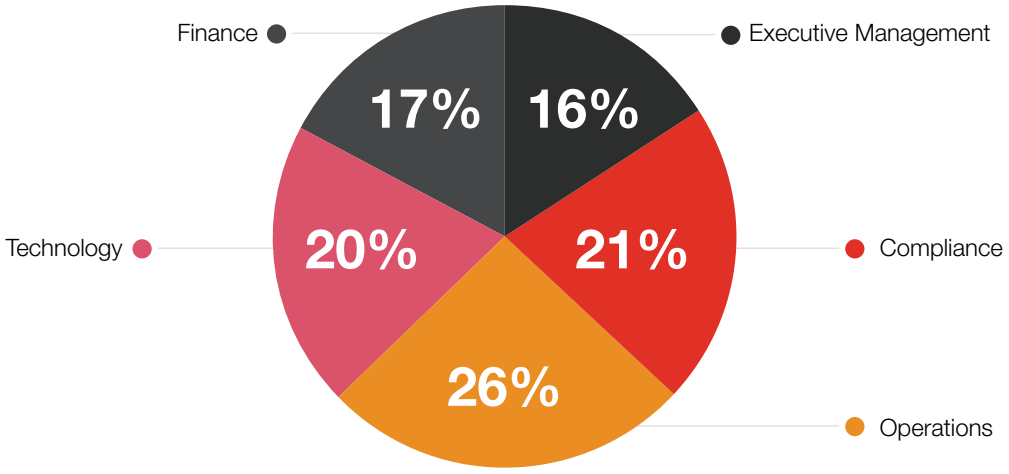
48% C-Suite Level

52% Others

When compared to the 2018 Singapore survey, more individual respondents are in Technology roles this year and fewer in Finance roles.

Technology roles		Finance roles	
2018	8%	2018	28%
2020	20%	2020	17%

Primary job functions of Singapore respondents



There was a varied industry mix amongst Singapore-based survey respondents.

- **Financial services, Banking and Capital markets** (20%)
- **Technology** (15%)
- **Consumer products and retail** (10%)
- **Engineering and construction** (9%)
- **Industrial products and manufacturing** (8%)
- **Energy, including oil and gas** (7%)
- **Others** (31%)

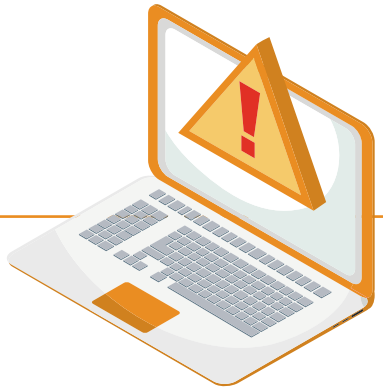
A higher proportion of Singapore-based respondents compared to global are from organisations with revenues over USD 5 billion.

Survey respondents with global revenue over USD 5 billion

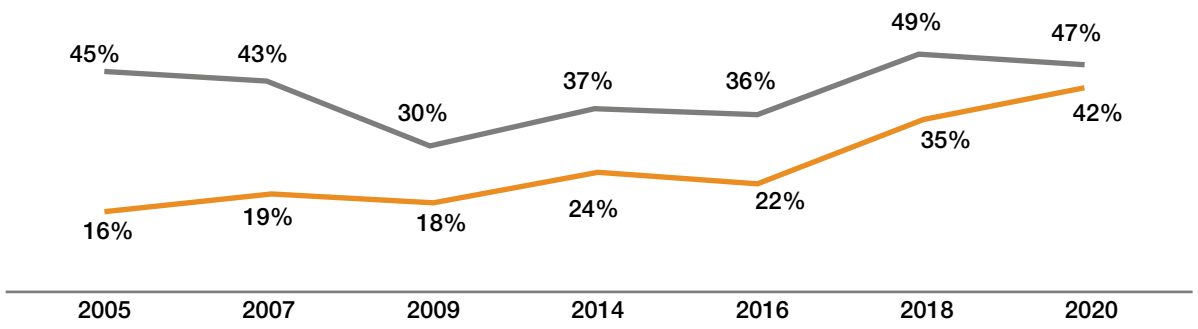
Singapore	Global
27%	17%

When fraud strikes: incidents of fraud

42% of Singapore-based companies experienced fraud over the last 24 months



Percentage of respondents experiencing fraud, corruption or other economic crime within the last 24 months



PwC's Global Economic Crime and Fraud Survey 2020 reveals that economic crime remains a persistent threat for Singapore-based companies: 42% of companies surveyed (compared with 47% globally) experienced incidents of fraud and economic crime within the past 24 months. This marks another record high for the country.

Despite its traditionally safe domestic environment, increasing exposure to global trends requires Singapore-based companies to face new threats.

Singapore's positioning as the financial hub for South East Asia and its role in catalysing international business flows within the region increasingly subjects Singapore-based companies to the risks inherent to operating in a dynamic cross-border environment. Singapore's regional exposure is likely to be one of the drivers of the growing reported economic crime rate.

Concurrently, a less favorable economic environment could also have impacted the observed trend. Typically, challenging economic conditions increase the pressure on employees to meet their key performance indicators, which may push them to commit fraud. Economic slowdowns also motivate companies to scrutinise their operations more closely which may result in detection of ongoing or past frauds.

In addition, heightened vigilance has led to increased discovery of economic crime, partially motivated by a crackdown on white-collar crime announced by the Singapore Police Force's Commercial Affairs Department (CAD) and the Monetary Authority of Singapore (MAS) in early 2018[1].

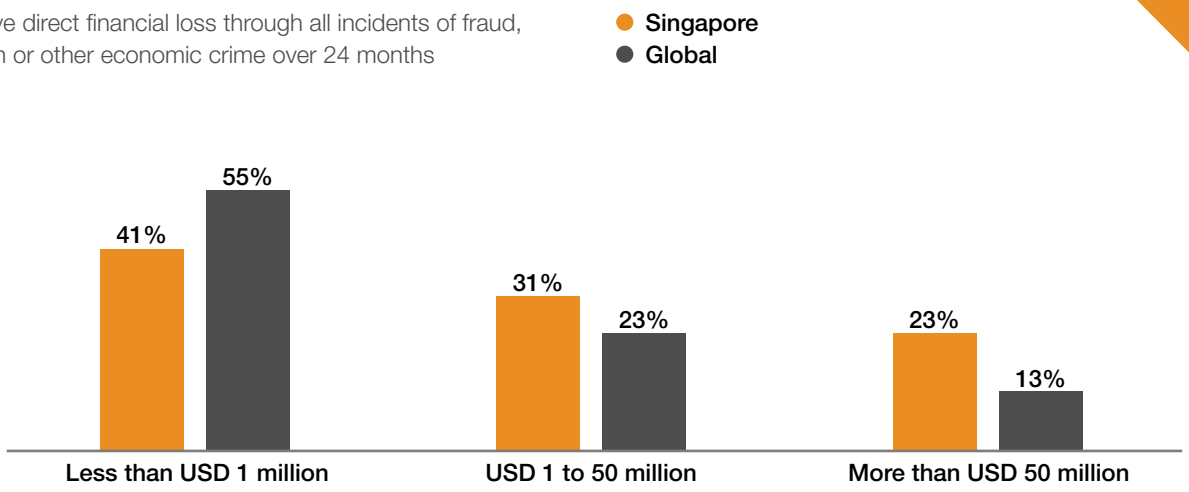
[1] https://www.bloomberg.com/news/articles/2018-01-18/meet-singapore-s-white-collar-crime-busters-quicktake-q-a

Cost of fraud

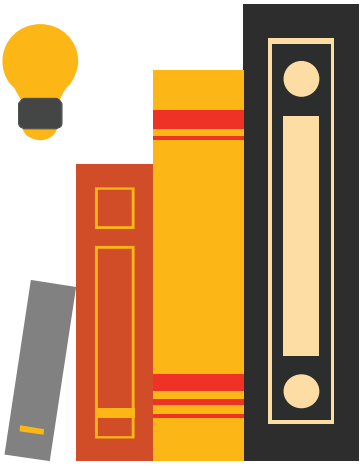
USD 50 M of cumulative losses reported by each of nearly a quarter of Singapore-based respondents

The majority (54%) of Singapore-based companies reporting fraud (compared to 36% globally) indicated that the cumulative direct financial impact of economic crime suffered during the last 24 months period was higher than USD 1 million. Of all companies reporting fraud, nearly a quarter (23%) of Singapore-based respondents (compared to 13% globally) indicated that their losses exceeded USD 50 million.

Cumulative direct financial loss through all incidents of fraud, corruption or other economic crime over 24 months



This situation may be partially explained by the fact that a higher percentage of Singapore-based survey participants belong to large organisations with revenue above USD 5 billion. Large companies typically report higher occurrence of economic crime due to their complex business operations. In Singapore, 53% of companies with revenue over USD 1 billion reported fraud and economic crime compared to only 29% for those with revenues below USD 500 million.

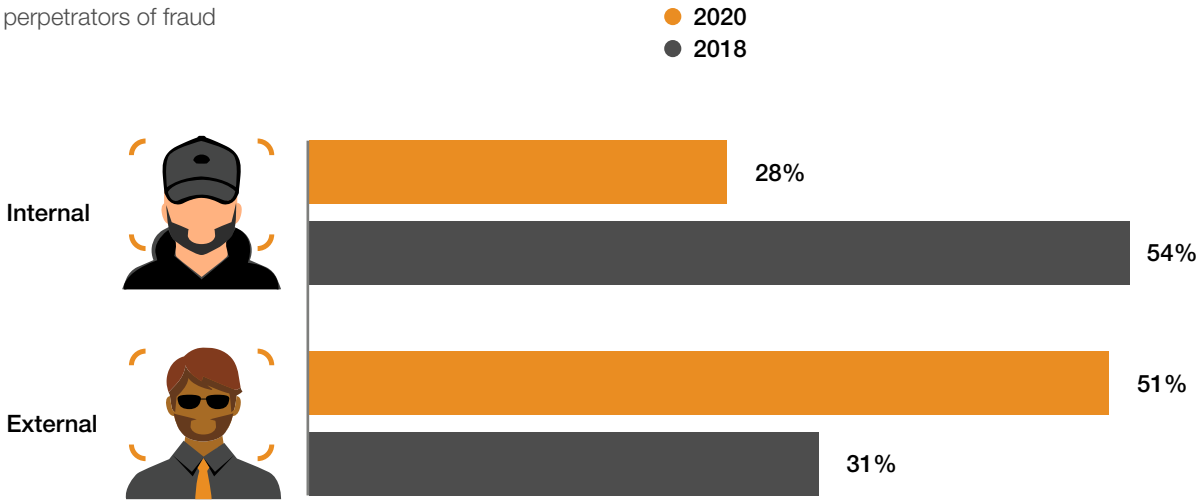


External fraud is on the rise

51% of frauds were committed by external perpetrators

Alongside the rising rate of economic crime, the survey results indicate a radical shift over the past two years in the main perpetrators of frauds suffered by Singapore-based companies from internal parties (28% in 2020 vs 54% in 2018) to more commonly being external parties (51% in 2020 vs 31% in 2018).

Main perpetrators of fraud

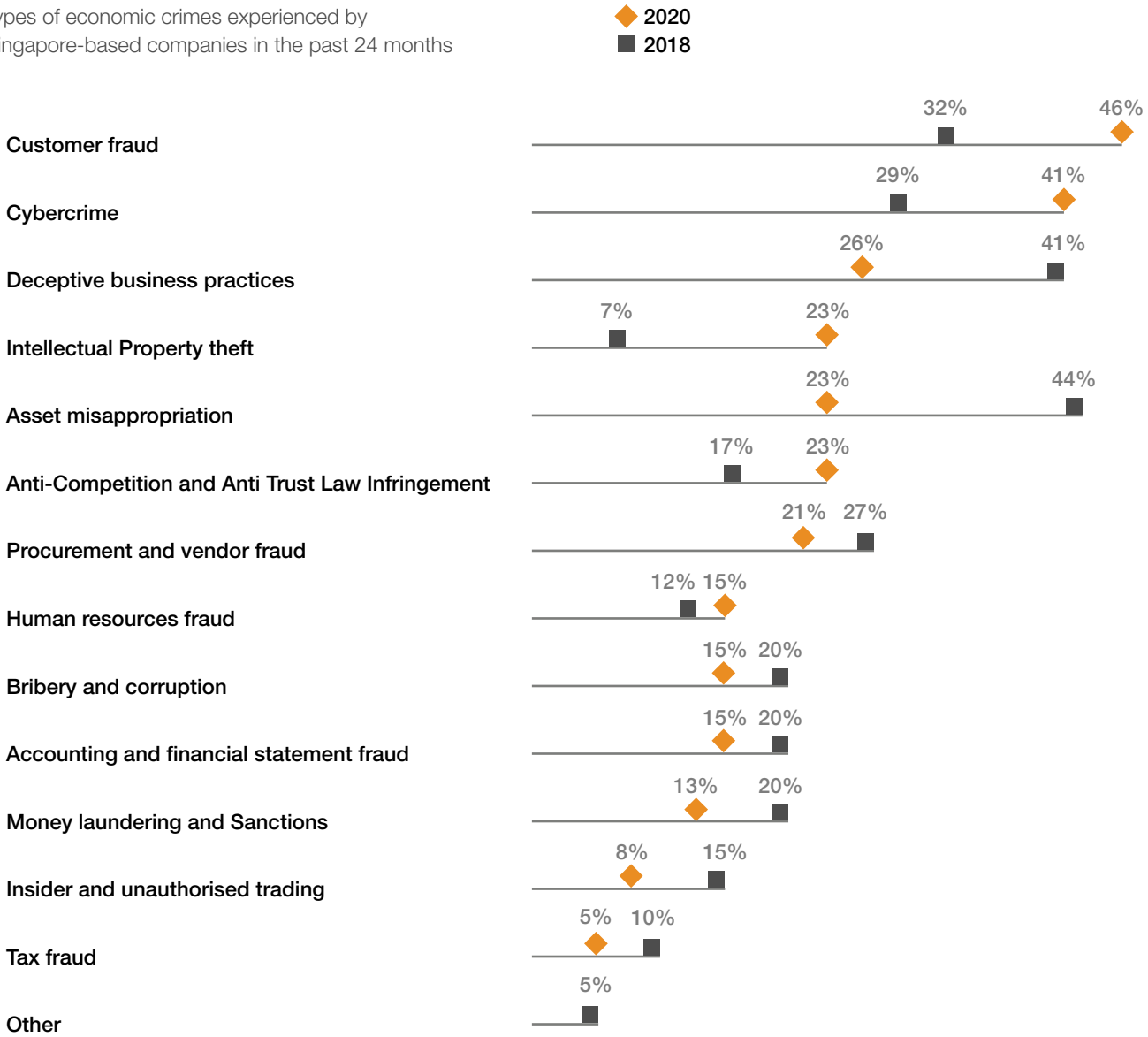


Customer Fraud was identified as the most prevalent economic crime (46%) followed closely by Cybercrime (41%) and Deceptive business practices (26%). Intellectual Property (IP) theft has also shown a substantial increase.

Addressing these new types of challenges requires a shift in focus from organisations. This may require bringing on board new sets of stakeholders and control mechanisms, especially as both Customer Fraud and Cybercrime were considered by survey respondents as the most disruptive and serious fraud incidents in their organisations.

At the same time, “traditional” white collar crimes, such as asset misappropriation, procurement fraud, accounting fraud, bribery and corruption are moderately decreasing. The decrease suggests that existing controls and prevention methods deployed by companies meaningfully contributed towards the reduction in the occurrence of these fraud incidents.

Types of economic crimes experienced by Singapore-based companies in the past 24 months



Cybercrime: Time to set tough guardrails in cyberspace

High-profile incidents widely publicised during the last 24 months both in Singapore and globally have emphasised the severity of the threat of cybercrime. From our experience, the increase in the incidence of cybercrime has been accompanied by an increase in the impact it has on organisations. The global average for the total cost of a single data breach rose to USD 3.92 million in 2019[2]. The financial services and technology industries have been heavily targeted due to the nature of their business.

Singapore-based companies are realising the value of implementing robust identity governance and administration to ensure that bad actors (internal or external) are unable to access key systems and data. Companies are also addressing the issue of data protection, which has risen to the top of the agenda. While regulations such as the Personal Data Protection Act (PDPA) in Singapore have focused on individual privacy, companies are increasingly seeing the need for systems to support data classification of current and legacy data. According to the 2019-2020 PwC Asia Pacific Business Leaders Survey, 83% of leaders in Singapore indicated that they wanted additional regulations in Cybersecurity.

In our experience, Singapore-based companies are ahead of their South East Asian counterparts in this area with 42% of Singapore-based companies having dedicated programmes to address cybercrime.

[2] https://www.ibm.com/security/data-breach

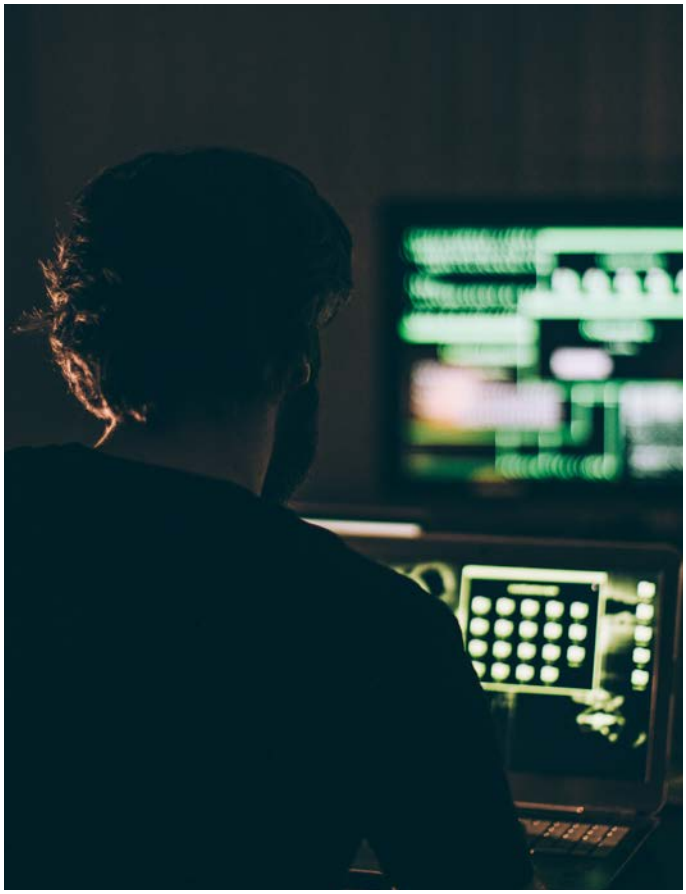
Bribery and corruption: compliance efforts pay off, but the threat remains

The perceived risk of domestic corruption remains low in Singapore, which ranks as the 4th least corrupt country in Transparency International's Corruption Perceptions Index[3]. The exposure of Singapore-based companies to the risk of bribery and corruption seems to be mainly related to their cross-border business activities.

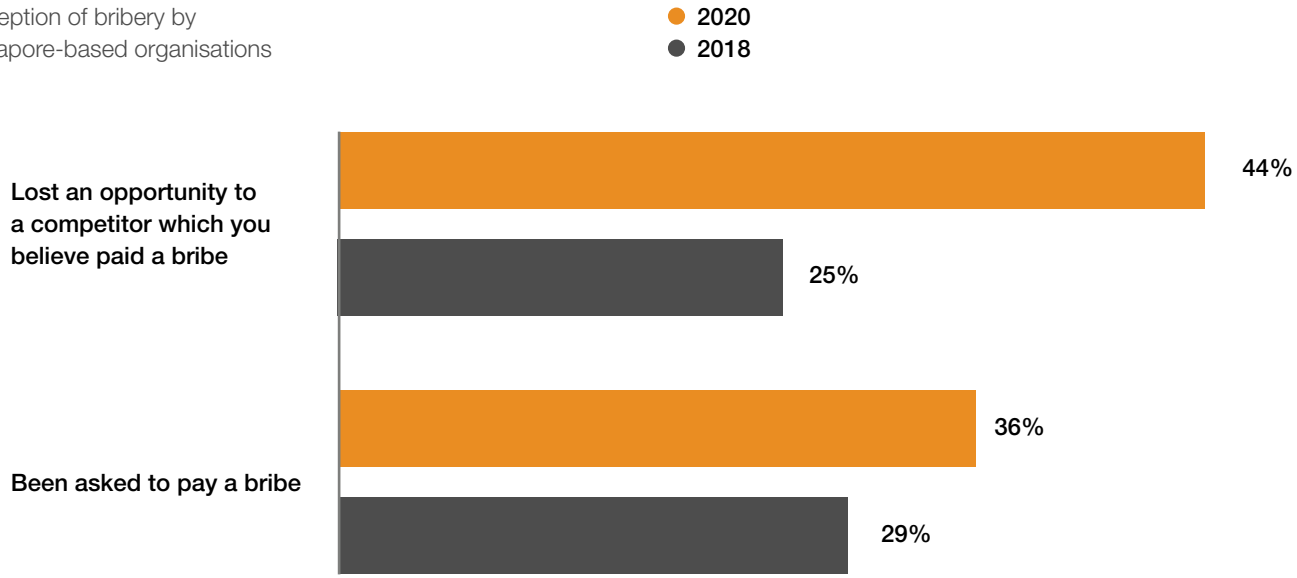
Positive news comes from the decrease of the reported incidence of bribery and corruption for Singapore-based companies from 20% in 2018 to 15% in 2020. This decrease is correlated with an increase in the proportion of companies with dedicated efforts on anti-bribery and anti-corruption compliance programs from 34% in 2018 to 38% in 2020.

At the same time, there are clear indications that the threat has not gone away: the global rate of bribery and corruption increased from 25% in 2018 to 30% in 2020 while the incidence rate in South East Asia increased from 29% in 2018 to 31% in 2020.

In this context, it is not surprising that an increasing proportion of Singapore-based companies reported that they have been asked to pay a bribe or had lost an opportunity to a competitor which they believe had paid a bribe.



Perception of bribery by Singapore-based organisations



[3] https://www.transparency.org/country/SGP

Behind the curve

39% of Singapore-based respondents have no formal risk assessment

Against the backdrop of a rising rate of fraud incidents reported by Singapore-based companies, some areas of internal risk management present an opportunity to improve fraud prevention and detection. This raises the question: are Singapore-based companies falling behind the curve?

Risk assessment

A well-conducted risk assessment helps a company to better understand and evaluate its specific risk exposure, develop plans to mitigate and manage risk as well as to better allocate resources. However, we note that 39% of Singapore-based survey participants do not have in place a formal risk assessment process.

28%

of Singapore-based respondents only conduct an informal risk assessment

11%

of Singapore-based respondents do not conduct any risk assessment

Policies, procedures and controls

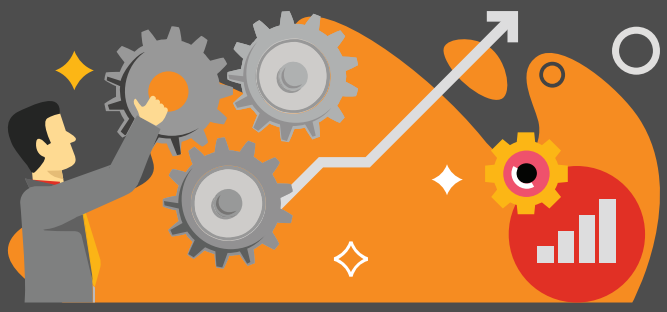
Formalised and well documented policies, procedures and controls are key to an effective internal control environment. However, 34% of Singapore-based survey participants reported that they do not have these elements in place.

27%

of Singapore-based respondents only have informal policies and procedures and some documented controls

7%

of Singapore-based respondents have no documented policies, procedures and controls



Third party management

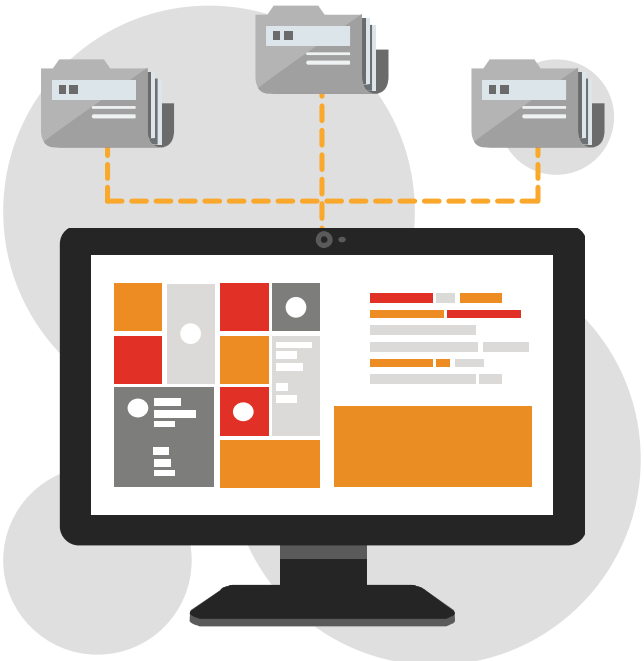
The substantial increase in external fraud brings under the spotlight risks inherent in dealings with third parties, whether it be customers, suppliers, service providers or contractors. Strikingly, 51% of Singapore-based participants indicate that they do not have formal risk-based due diligence and an ongoing monitoring process in place for third parties.

41%

of Singapore-based companies employ informal risk-based due diligence and ongoing monitoring for third parties

10%

of Singapore-based companies do not conduct any third-party assessment



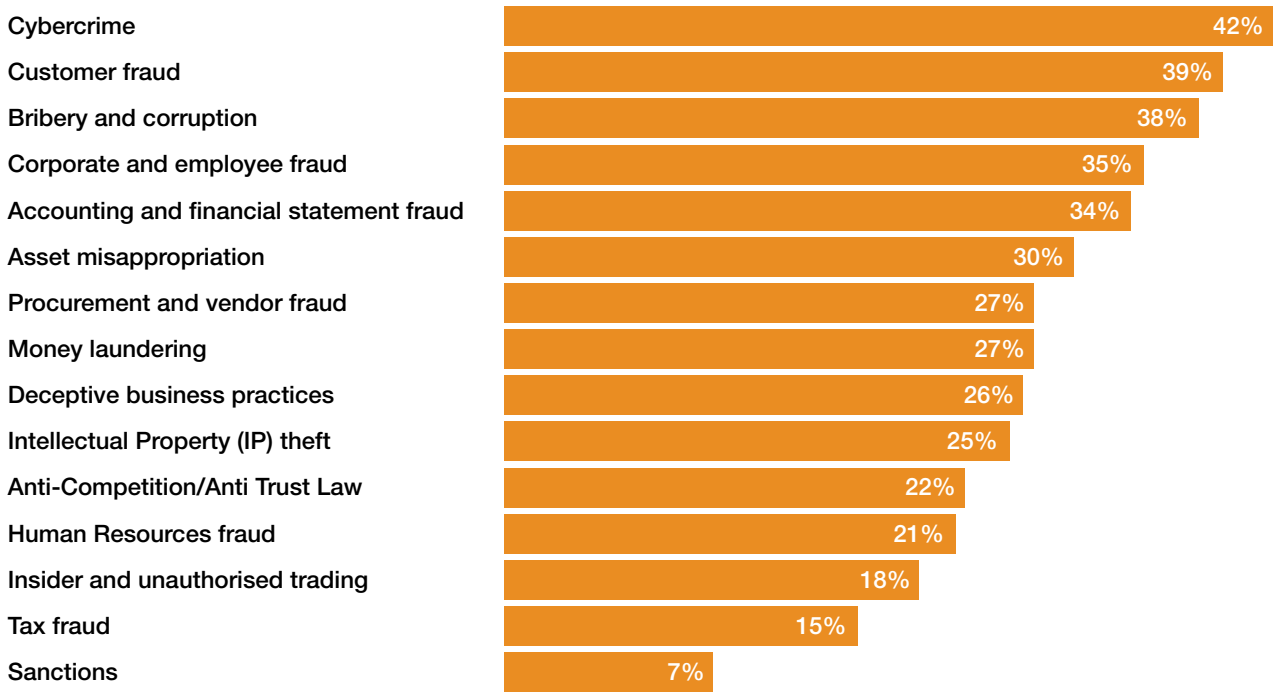
Dedicated fraud risk management programs

The level of adoption of dedicated fraud risk programmes by Singapore-based companies is broadly similar to the global average. Overall, there is still significant potential for the creation of dedicated fraud risk management programmes to help companies to address the areas of highest risk.

The way forward:

1. Build a robust risk assessment as the foundation of a successful risk management programme
2. Formalise the response to fraud risk to better mitigate and manage risk
3. Create dedicated fraud risk management programmes to address areas of highest risk

Percentage of Singapore-based companies with a dedicated programme to address



Harnessing technology to combat fraud

3 out of 4 respondents in Singapore have upgraded their technology used to combat fraud

Companies have long recognised the potential of technology to enhance their internal control systems. In Singapore, suspicious activity monitoring is the leading detection mechanism of fraud incidents (23%), almost two times higher than the global average (12%).

The use of advanced technology in Singapore is approximately similar to the use within the region and globally. However, Singapore-based organisations are more mature in their use of Artificial Intelligence with 23% of companies using it and finding value, as compared to the global average of 16%.

We found that nearly 3 out of 4 (73%) respondents in Singapore implemented or upgraded the technology used to combat fraud, corruption and economic crime over the past two years.

21%

of Singapore-based companies have real-time detection/alert generation for fraudulent activities in addition to regular testing for operating effectiveness

15%

of Singapore-based companies conduct risk based due diligence and ongoing monitoring of third parties enabled through the use of web-based applications and other tools and technology

At the same time, the rate at which companies are using advanced technology to support their risk management is still relatively low and there is potential to enhance internal control systems through the use of technology.

Crucially, we observe a significant degree of variation in the value each company is able to derive from different technologies. Better customisation of appropriate technological solutions to specific risks faced by each organisation can help to find value-added solutions for adoption.

The differences in the value that companies are able to find from technology tools also underline the importance of the quality of the associated implementation process. In relative terms, companies often dedicate more efforts to the introduction of these technologies with less attention paid to continuous maintenance, which is important to derive value on a long-term basis.

The way forward:

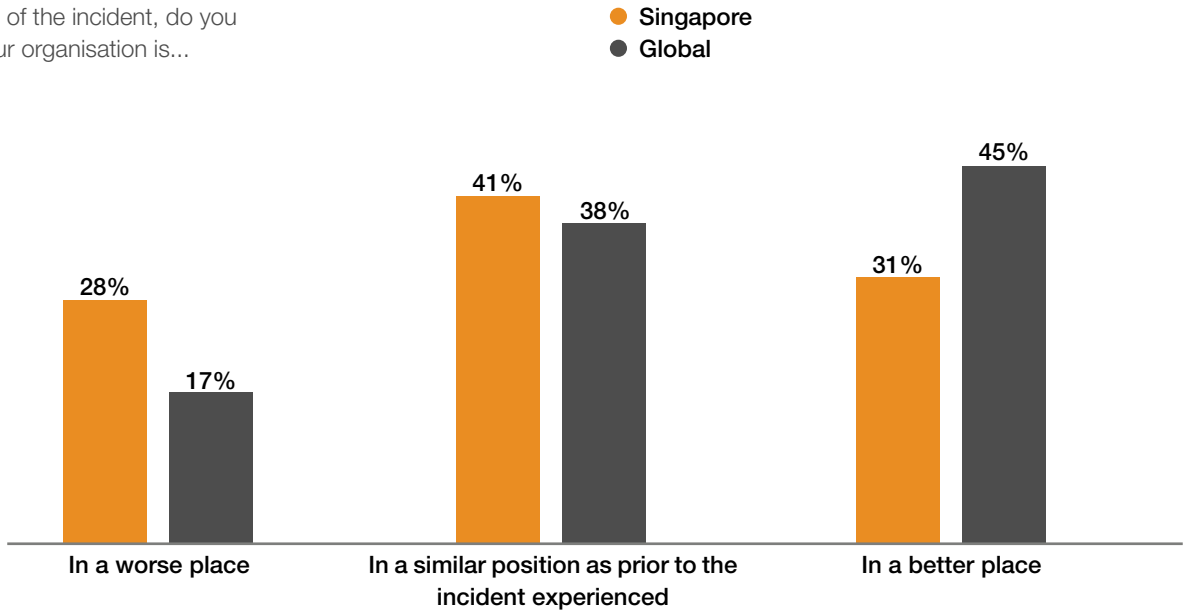
1. Investing in strategic technology is a necessary but not sufficient condition for a successful risk management programme
2. To obtain value, technology must be customised to fit the specific risks, needs, and capabilities of each organisation
3. To remain effective, continuous maintenance is critical

Missing an opportunity

Less than 1 in 3 Singapore-based companies feel they are in a better position after experiencing and remediating a fraud

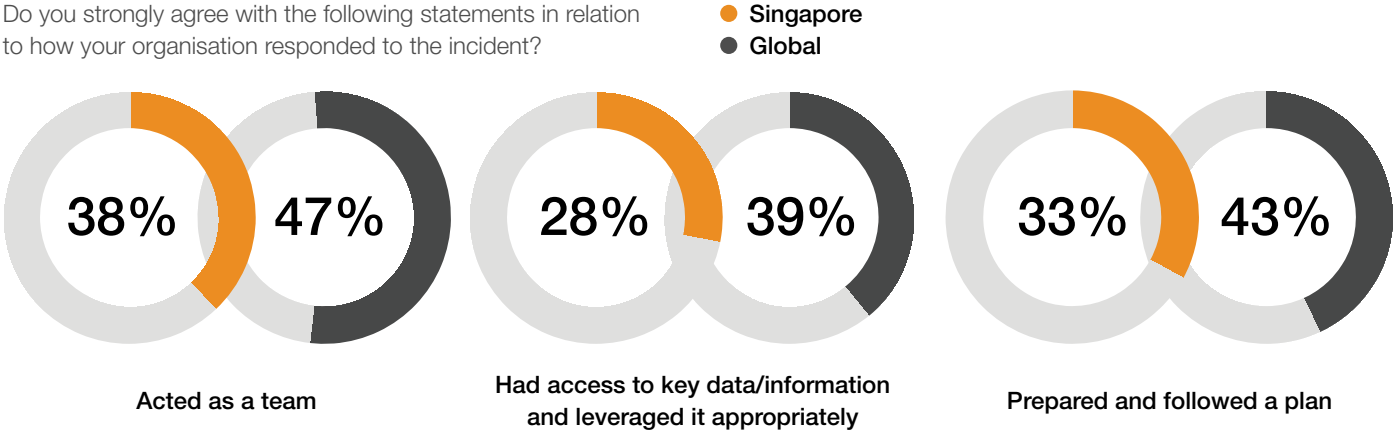
Economic crime is a reality for many companies. Each fraud incident is a stressful event for an organisation, but also an opportunity to improve its control environment and to emerge stronger.

As a result of the incident, do you believe your organisation is...



In this respect, 45% of companies globally said that, as a result of the incident that occurred, they felt their organisations were in a better place compared to only 31% of Singapore-based survey participants. A higher proportion of companies in Singapore (28% vs 17% globally) felt they were in a worse place.

Do you strongly agree with the following statements in relation to how your organisation responded to the incident?



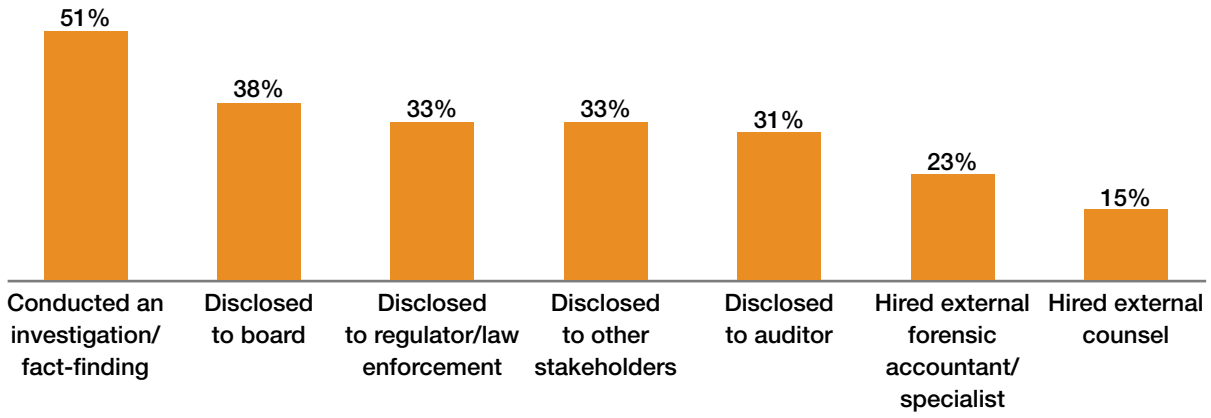
The survey results suggest that organisations in Singapore are likely to feel they were in a worse place after the incident due to the nature of their organisational responses. A lower proportion of Singapore-based participants, as compared to the global average, strongly felt that their organisation came together as a team and followed a well-developed plan to address the incident. Improving access to key data and information to support investigation efforts would also allow companies in Singapore to emerge stronger.

Are the responses of companies to economic crime sufficient in preventing recurrence? Our results show that 49% of respondents did not conduct an investigation after an incident occurred. This would typically limit the analysis of root causes of the incident and reduce the effectiveness of other responses such as changes to policy, governance and controls. Companies that do not conduct an investigation are more exposed to the risk of reoccurrence of an incident.

The way forward:

1. View disruptive events as an opportunity for forward-looking transformation
2. Understanding the root causes of incidents is critical
3. Formulating and executing structured responses to a fraud incident appears to be a key element for an organisation to emerge stronger

How did organisations respond to incidents?



Contacts

Michael Peer
Forensics Leader
PwC Singapore
+65 9663 9089
michael.peer@pwc.com

Richard Major
South East Asia Risk Consulting Leader
PwC Singapore
+65 6236 3058
richard.j.major@pwc.com

Nick Davison
Financial Crime Unit Leader
PwC Singapore
+65 9732 7330
nick.davison@pwc.com

Kheng Tek Chan
Business Recovery Services Partner
PwC Singapore
+65 6236 3628
kheng.tek.chan@pwc.com

David Toh
Internal Audit Leader
PwC Singapore
+65 6236 3248
david.sh.toh@pwc.com

Dmitry Kosarev
Forensics Director
PwC Singapore
+65 9671 1326
dmitry.kosarev@pwc.com

pwc