Under attack: are organisations doing enough to tackle the cyber threat?
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Subtitle</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Foreword</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>The global landscape</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>The local landscape</td>
<td></td>
</tr>
</tbody>
</table>
| 4       | Hong Kong and Macau | Corporate cyber security: fit for purpose?  
AML progress hindered by recruitment difficulties |
| 8       | Mainland China | Change: the only constant in the compliance world  
Organisations still stalked by the ‘danger within’ |
| 12      | PwC final thoughts | The next challenge for compliance in mainland China |
| 13      | Methodology and statistics highlights |          |
| 14      | Contacts |          |
Welcome to PwC’s Global Economic Crime Survey 2016 (GEC Survey, the Survey) – mainland China, Hong Kong and Macau Supplement (the Supplement). Drawn from PwC’s biennial GEC Survey which is based on more than 6,300 respondents from 115 jurisdictions and territories worldwide, this Hong Kong, Macau, and mainland China Supplement addresses the corporate experience and response to economic crime based on an online survey of nearly 200 senior business people who live and work in these markets. It also marks the second consecutive supplement to include distinct sections focusing on Hong Kong and Macau and on mainland China, making the Supplement one of the most comprehensive of its kind leveraging statistical comparisons based on year, jurisdiction, and subject matter.

How much has changed during the last two years and what has remained constant? As with previous years, misappropriation (or theft) of assets – usually the easiest economic crime to detect and therefore also the most widely reported – was ranked the most commonly experienced economic crime both by respondents in mainland China and in Hong Kong and Macau. Other trends and developments, however, can be equally harmful to organisations, especially to those with compliance and/or IT departments which are ill prepared to meet changing conditions.

Aside from asset misappropriation, the Supplement’s dominant themes in Hong Kong and Macau as reported by respondents are cybercrime and money laundering, and how effectively organisations are meeting these challenges. Frequently in the headlines during the last 24 months, often as a result of Hong Kong (and global) regulators’ anti-money laundering (AML) enforcement actions, these two types of crimes are especially relevant to a technology-dependent financial hub like Hong Kong and a major gaming centre like Macau, and are also major themes in the PwC Global Economic Crime Survey 2016.

In mainland China, the focus moves to bribery and corruption – never far from the news as the PRC’s anti-corruption campaign enters its fourth year under President Xi Jinping with few signs of slowing down. The Supplement also looks at findings relating to procurement fraud, a perennial challenge faced by organisations in mainland China.

In most instances, the findings corroborate what we hear directly from industry and supports PwC’s own first-hand experience. In all instances, we try to help the reader make sense of the findings by providing context, by making observations based on what we see on the ground, and by making suggestions as to what can practically be done to address the issues raised.

John Donker
Lead Partner, PwC China & Hong Kong Forensic Services
The global landscape

Top 3 most commonly reported types of economic crime in 2016

- Asset misappropriation: 64%
- Cybercrime: 32%
- Bribery and corruption: 24%

Types of economic crime experienced

- Asset misappropriation: 64% (2016), 69% (2014)
- Cybercrime: 32% (2016), 24% (2014)
- Bribery and corruption: 24% (2016), 27% (2014)
- Procurement fraud: 23% (2016), 29% (2014)
- Accounting fraud: 18% (2016), 22% (2014)
- Human resources fraud: 12% (2016), 15% (2014)
- Money laundering: 11% (2016), 11% (2014)
- IP infringement: 7% (2016), 8% (2014)
- Insider trading: 7% (2016), 4% (2014)
- Tax fraud: 6% (2016), 6% (2014)
- Mortgage fraud: 6% (2016), 7% (2014)
- Competition/anti-trust law infringement: 4% (2016), 5% (2014)
- Espionage: 2% (2016), 3% (2014)
- Other: 14% (2016), 11% (2014)

Which industries are at risk?

- Financial Services: 48%
- Global Economic Crime Rate: 36%
- Technology: 44%
- Hospitality & Leisure: 29%
- Professional Services: 37%
- Pharmaceuticals & Life Sciences: 37%
- Energy, Utilities & Mining: 37%
- Engineering & Construction: 33%
- Manufacturing: 32%
- Entertainment & Media: 29%
- Insurance: 29%
- Aerospace & Defence: 43%
- Communications: 42%
- Retail & Consumer: 43%
- Manufacturing: 43%
- Engineering & Construction: 38%
- Energy, Utilities & Mining: 37%

Note: The percentages in the diagram are illustrative and do not necessarily reflect the exact values shown in the table.
The local landscape

Highlights

28% (27% in 2014) of respondents in mainland China and 21% (16% in 2014) in Hong Kong and Macau report that they have experienced economic crime, compared to 30% (32% in 2014) in Asia Pacific and 36% (37% in 2014) globally.

<table>
<thead>
<tr>
<th>Mainland China</th>
<th>Hong Kong and Macau</th>
</tr>
</thead>
<tbody>
<tr>
<td>35% of respondents in mainland China said they didn’t know how often in the last 24 months their organisations had performed a fraud risk assessment</td>
<td>Dominant themes in Hong Kong and Macau are cybercrime and money laundering</td>
</tr>
<tr>
<td>63% of respondents in mainland China who had experienced economic crime said that the most serious losses were perpetrated by the “insider”</td>
<td>50% of respondents in Hong Kong and Macau who reported suffering from economic crime claimed to have experienced cybercrime</td>
</tr>
<tr>
<td>38% of mainland China-based respondents said they thought their organisation will experience bribery and corruption in the next 24 months, compared to 14% in the United States and a BRICS average of 35%</td>
<td>43% of respondents in Hong Kong and Macau claimed the ability to hire experienced staff was a significant challenge in relation to complying with local AML/CFT requirements</td>
</tr>
<tr>
<td>22% of respondents in mainland China said they had been asked to pay a bribe in the last 24 months. 36% believed that their organisation had lost out to a competitor who had paid a bribe</td>
<td>24% of Hong Kong and Macau respondents said their companies lost more than US$50,000 through cybercrime</td>
</tr>
</tbody>
</table>

According to the respondents who claimed to have experienced procurement fraud in mainland China, fully 100% said it had occurred during the vendor selection process and 80% during vendor contracting.

Only 13% of mainland China-based respondents who had experienced economic crime during the last 24 months said that they had encountered cybercrime. This is down from 22% in 2014.

14% of respondents in Hong Kong and Macau thought reputational damage was the most serious impact through cybercrime.

32% of respondents in Hong Kong and Macau claimed systems generating false positive alerts as a significant challenge.

Types of Fraud

- Global
- Asia Pacific
- Mainland China
- Hong Kong and Macau
Awareness of the threat of cybercrime has also increased. Just over half (51%) of Hong Kong and Macau-based respondents said that they perceived the risk of cybercrime to have increased during the last 24 months, rising from 39% in 2014 and in line with a global average of 53%. PwC’s Global State of Information Security Survey 2016 (GSISS)1 – which includes 330 responses from Hong Kong, Macau, and mainland China – shows that the combined number of security incidents (defined as an event that threatens some aspect of an organisation’s computer security) in 2015 in Hong Kong and China dramatically increased by a multiple of five over 2014. (Note that a ‘security incident’ does not necessarily mean that a breach has taken place; only that an attack has occurred.)

Of note, cyber-attacks and incidents in the region are on the rise. Some 50% of respondents who reported suffering from economic crime claimed to have experienced cybercrime, up from 37% in 2014, and higher than the global average of 32%. Of these instances, over 76% of respondents said their organisations experienced service disruptions affecting consumers, and more than two thirds said they believed these incidents had a moderate to high negative impact on the organisation’s brand reputation.

Awareness of the threat of cybercrime has also increased. Just over half (51%) of Hong Kong and Macau-based respondents said that they perceived the risk of cybercrime to have increased during the last 24 months, rising from 39% in 2014 and in line with a global average of 53%. PwC’s Global State of Information Security Survey 2016 (GSISS)1 – which includes 330 responses from Hong Kong, Macau, and mainland China – shows that the combined number of security incidents (defined as an event that threatens some aspect of an organisation’s computer security) in 2015 in Hong Kong and China dramatically increased by a multiple of five over 2014. (Note that a ‘security incident’ does not necessarily mean that a breach has taken place; only that an attack has occurred.)

1PwC’s Global State of Information Security Survey 2016 (GSISS) is an annual survey of more than 10,000 senior executives from 127 countries and territories.
The need to tighten IT security

Although many financial and banking institutions are at the forefront of cybersecurity developments and advancements given that they are high-value targets for cybercrime, more needs to be done around existing procedural tasks such as accountability, periodic security control reviews, systems monitoring, and incident response. As such, the Hong Kong Monetary Authority (HKMA) issued guidance in September 2015, outlining the need for financial institutions to revisit their cyber risk management procedures, regularly update incident response strategies, and provide technical know-how to respond to any organisational security incident, as part of a broader effort to tighten their IT security.

Despite these efforts, however, findings from the GEC Survey suggest that there remain a number of question marks over Hong Kong’s broader business community’s awareness of cybercrime, of its impact on their organisations, and of how to tackle it – though many responders recognise it as a concern. One in five respondents who experienced cybercrime were unsure of the economic impact on their respective organisation, and 40% of Hong Kong and Macau-based respondents said that their Board members do not request, or have not considered the need to request information regarding their organisation’s state of readiness to deal with cyber incidents.

Additionally, according to findings from the GSISS (in which 75% of Hong Kong, Macau and mainland China respondents were from IT-related backgrounds), 46% of respondents said that their Board members did not actively participate in overall cybersecurity strategy. Does this then mean that senior management are not always setting the appropriate ‘tone at the top’ with regard to cybersecurity, or that Board members overwhelmingly still regard cybersecurity as an issue best left for IT and technology departments to address? Or does it mean that senior leaders still do not sufficiently understand the risk of cybercrime?

How often do Board members request information regarding the organisation's state of readiness to deal with cyber incidents?

- 5% Monthly
- 13% Quarterly
- 12% Annually
- 31% Board members do not request this information
- 9% Board members have not considered the need for this information
- 5% Other
- 26% Don’t know

“40% of Hong Kong and Macau-based respondents said that their Board members do not request, or have not considered the need to request information regarding their organisation’s state of readiness to deal with cyber incidents.”
This (over)confidence in organisations’ state of readiness seems to be widespread. Just under half (49%) of Hong Kong and Macau-based respondents said that their organisations would be unlikely to experience cybercrime during the next 24 months. Additionally, 53% said their organisations lacked internal or external first responders trained to react to a technology breach, while only 38% said that their organisations had incident response plans.

Perhaps of greatest concern is the lack of awareness of the real origin of the cyber threat. 62% of Hong Kong and Macau-based respondents believe that any cybersecurity incident occurring within the next 24 months would most likely originate from an external source. By contrast, 1% believed that the most likely threat in the next 24 months would come from an inside actor. Findings from the GSISS note, however, that 50% of incidents reported originated from insider-related events involving current and former employees.

Given that the damage caused by large-scale theft of customers’ personal and credit card details can be just as damaging to organisations as financial losses (and perhaps even more so given the publicity that usually surrounds such breaches), organisations across Hong Kong and Macau may still need to do more to assess and safeguard their most prize assets and make sure they have an incident response plan ready.

In the short term, making sure that existing security teams are adequately trained and staffed to respond to attacks, and that security awareness culture in the workplace is robust, should take precedence over attempting to fix the problem with a new IT security solution, especially if systemic issues in workplace processes and procedures can be identified. In the longer term, providing senior management with data analytics-based dashboards to review cybersecurity reports will improve workplace awareness and strengthen an organisation’s overall security posture and culture.

“In the longer term, providing senior management with data analytics-based dashboards to review cybersecurity reports will improve workplace awareness and strengthen an organisation’s overall security posture and culture”
AML progress hindered by recruitment difficulties

No survey would be complete without an unexpected result or two. Only 10% of Hong Kong and Macau-based respondents said that their organisations had encountered money laundering during the last 24 months, a steep fall from 37% two years ago. Increased regulatory enforcement of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (AMLO) by the HKMA and the Securities and Futures Commission (SFC) may go some way to explaining this fall in reported money laundering, prompting financial institutions to invest heavily in AML/combatting the financing of terrorism (CFT) capabilities and to significantly tighten their ‘know-your customer’ (KYC) and transaction monitoring procedures. Extensive and ongoing ‘de-risking’ by banks has also seen them move away from many of their riskier clients.

Encouraging though this finding may be, the GEC Survey gauges corporate experience from across a range of industries and is not solely focused on financial services (though this was the most represented industry accounting for 32% of respondents in Hong Kong and Macau, followed by the retail/consumer and the manufacturing industries at 13% and 12% respectively). In a pulse survey taken at a major compliance summit in Hong Kong last year, an audience of almost 400 senior executives overwhelmingly drawn from the financial services industry was asked ‘which regulation is the biggest concern for your business?’ Money laundering came out on top with 61% of the vote.

The Supplement also sheds light on the shortage of experienced compliance personnel staff with 43% of Hong Kong and Macau-based respondents citing staffing resources as a ‘significant challenge’ (compared to 19% in Singapore, 16% in the US, and a global average of 19%). This is particularly significant given Hong Kong and Macau-based organisations’ dependence on transaction monitoring systems (TMS), with 61% of respondents who claimed to have encountered economic crime saying that their organisation identified suspicious activities using these automated scenario-based monitoring systems. Though these systems can be effective (as 32% of respondents claim), they also need to be supported with sufficient staff and resources to keep them up-to-date with the latest technology and techniques. Failure to do so can result in these systems generating too many false positive alerts, which 32% of respondents claimed was a significant challenge in relation to AML/CFT programs.

---

2 Hosted by Haymarket Financial Media, the ‘4th Annual Compliance Summit Asia’ was held in Hong Kong on November 10, 2015. PwC was the lead sponsor.
Overall crime as reported by mainland China-based respondents in the 2016 Supplement remained broadly consistent at 28% with the 2014 Supplement’s 27%, and less than the average of the BRICS countries (Brazil, Russia India, China, and South Africa) at 39%. As with the previous Supplement, bribery and corruption remains one of the key concerns for organisations in mainland China, not least because of the well documented enforcement actions from US regulators – and increasingly from PRC regulators – against public sector officials and personnel at both local companies and multinational corporations.

It would therefore be surprising if bribery and corruption did not feature strongly in the Supplement, and sure enough, 46% of mainland China-based respondents cited it as the most commonly encountered economic crime, up from 39% in 2014. While the number of mainland China-based respondents who said that they had been asked to pay a bribe fell from 27% in 2014 to 22% in 2016, 36% said that they believed that during the last 24 months their organisation had lost out to a competitor who had paid a bribe (compared with 8% in the US and a BRICS average of 19%). In addition, 38% of mainland China-based respondents said they thought that their organisation will experience bribery and corruption in the next 24 months, compared to 14% in the US and a BRICS average of 35%.

In the last 24 months, has your organisation lost an opportunity to a competitor which you believe paid a bribe?

- **36%** Yes
- **44%** Don’t know
- **20%** No
It is probably the case, however, that the more organisations look for indications of suspicious activity the more they will find. In other words, increased reporting of an economic crime may well be a result of more effective identification processes than of an increase in occurrences. Greater numbers of organisations are, for example, investing in highly adaptable dashboard-based data analytics and data visualisation technology to help them more efficiently identify suspicious transactions and behaviour, as PwC has seen during recent years.

This is not to underestimate the seriousness of the threat posed to organisations by bribery and corruption in mainland China. Transparency International’s Corruption Perception Index 2015, which measures perceived levels of public sector corruption, ranked China in equal 83rd position out of 168 countries and territories with a score of 37 (where 0 is considered to be highly corrupt and 100 very clean). Despite this improvement over the 2014 index where China was ranked 100th with a score of 36, the Corruption Perception Index and the GEC Survey should still reinforce the need for organisations to make sure their compliance personnel, procedures, and business cultures are adequate to meet a dynamic and high-stakes regulatory environment.

**Organisations still stalked by the ‘danger within’**

The 2016 Supplement in part echoes findings from the 2014 Supplement, entitled ‘The Danger Within’. The Supplement of two years ago highlighted the risk posed by the ‘insider’ and how the actions of employees and former employees could leave their organisations exposed to serious financial loss and/or regulatory sanction if left unchecked and if organisations failed to effectively monitor their dealings with third parties. Though down from 78% in 2014, 63% of respondents to the 2016 Survey who had experienced economic crime still said that the most serious of such losses were perpetrated by a member of staff (compared to 29% in the US, a BRICS average of 50%, and a global average of 46%). Altogether, 53% of respondents who claimed their organisations had encountered economic crime said that middle management was responsible for the most serious monetary losses, while 38% said that perpetrators of the economic crime were between 31 and 40 years old. Finally, 31% said that the perpetrator of the fraud had worked at the company for between six and 10 years.
Faced with this level of employee fraud risk, organisations’ compliance programs need to include codes of conduct (made widely available to employees in Chinese) and a response plan in the event that an organisation receives an allegation. Organisations also need to be able to continuously monitor transactions and third parties for suspicious activity and red flags.

Procurement fraud, for instance, was widely reported by respondents in the 2014 GEC Supplement as a major challenge to business, not least as lack of insight into third parties and intermediaries has been a major driver of many FCPA investigations by US regulators.

Based on PwC’s clients’ experience in mainland China, procurement fraud – including collusion with intermediaries such as travel agents providing fake documentation to support fictitious events, and kickback schemes using friends and family as bogus vendors – is often supported by fraudulent documentation including fake contracts, tax receipts, and credit card slips from black market vendors. These can render organisations vulnerable to regulatory enforcement action, not to mention create serious pricing and quality risks.

However, instances of procurement fraud as reported by respondents who experienced economic crime fell sharply to 21% in 2016, from 48% in 2014 (though it was still ranked as the third most commonly reported economic crime in mainland China closely followed by accounting fraud). One explanation for this unexpectedly low result may be that compliance departments are now so focused on anti-bribery and corruption efforts that they are recording different types of fraud (including procurement fraud) under the ‘bribery and corruption’ category. Note that procurement fraud is often a favoured means used by fraudsters to extract cash from an organisation to fund payment of bribes to improperly secure contracts and win business.

Another explanation may relate to the number of recent high-profile enforcement actions undertaken by PRC and US authorities, focusing organisations’ attention on the importance of effective compliance, especially with regard to behaviour of opaque third-party networks and agents.
This decrease in reported instances of procurement fraud could also be evidence of creeping complacency. When asked, 35% (compared to 11% in 2014) of respondents said they were unaware of how often in the last 24 months their organisations had performed a fraud risk assessment in mainland China (compared to global, Asia Pacific, and BRICS averages of 18%, 19%, and 17% respectively). 62% of respondents also said that their organisations had not increased compliance spending during the last two years, with 55% saying that they did not expect increased investment during the next 24 months.

The same specific challenges within the procurement process also seem to have remained fairly constant. According to the 2016 findings, of the respondents who claimed to have experienced procurement fraud, fully 100% said it had occurred during the vendor selection process and 80% during vendor contracting, compared to 91% and 55% in 2014 respectively. So the same weaknesses relating to procurement fraud identified in the Supplement in 2014 remain major concerns two years down the line, again bringing into question whether organisations are doing enough to understand and monitor their third-party networks.
Sometimes surveys are as interesting for what they don't say as much as for what they do. There is little doubt, for instance, that the PRC’s anti-corruption drive is raising business awareness of bribery and corruption across the nation. Experienced compliance personnel have never been in greater demand, compliance-themed conferences and events are usually packed, and organisations are trying to invest in larger and more sophisticated compliance departments, despite a chronic shortage of qualified personnel.

However, two economic crimes appear to be slipping below the radar, at least according to findings of this Supplement. Not one mainland China-based respondent cited having encountered instances of money laundering during the last 24 months, begging the question whether employees know what to look for.

Additionally, only 13% of mainland China-based respondents who had experienced economic crime during the last 24 months said that they had encountered cybercrime, noting that the heaviest impact related to theft of intellectual property and of personal details. Online retail is a daily feature in the lives of many ordinary Chinese people, who order a wide range of products online or by smartphone, from groceries and take-away food to household furniture and electronic goods. Anecdotal instances of online card fraud are by no means unusual, and anyone with a bank account will regularly receive text messages warning them of the dangers of ‘social engineering’ and ‘phishing’, and to be extremely careful of divulging sensitive information to possible fraudsters.

According to the GSISS, the financial impact on companies globally from cyber security incidents have slightly decreased by 5%, but have increased in Hong Kong and China by 10%. Given that China boasts some of the largest online marketplaces in the world, and given how quickly China has taken to e-commerce, organisations might do well to ask themselves some hard questions as to whether they really are on top of this situation, or whether they need to be doing more to secure themselves against the risk of money laundering, social engineering, and cybercrime.
Methodology and statistics highlights

PwC carried out the Global Economic Crime Survey between July 2015 and September 2015. The aim of the Survey is to assess corporate attitudes to fraud in the current economic environment, and particularly to understand how organisations are responding to incidents of cybercrime-related fraud, the prevalence of bribery/corruption and money laundering and the effect these are having on organisations’ business ethics and compliance programmes, and what types of fraud are most common.

The Survey consisted of a globally accessible web based questionnaire on a secure site. Executives wishing to respond to the Survey were directed to the site, and responded to the following sections:

- General profiling questions
- Economic crime trends
- Technology – an economic crime blessing or curse?
- Profile of the fraudster and detection methods
- Business ethics and compliance programs

### Respondents profile

- **35%** of mainland China respondents were C-suite
- **56%** of HK & Macau respondents were C-suite
- **65%** in mainland China of respondents were managing the Finance, Executive Management, Audit, Compliance and Risk Management Functions
- **87%** in HK & Macau
- **59%** in mainland China of respondents employed by organisations with more than 1,000 employees
- **59%** in HK & Macau
- **48%** in mainland China of respondents were heads of department or business units
- **31%** of HK & Macau respondents were heads of department or business units
- **48%** in mainland China of the survey population represented Publicly Traded Companies
- **49%** in HK & Macau

### Industry sectors

- **18%** in mainland China
- **12%** in HK & Macau
- **Manufacturing**
- **14%** in mainland China
- **32%** in HK & Macau
- **Financial Services**
- **11%** in mainland China
- **3%** in HK & Macau
- **Technology**
- **9%** in mainland China
- **1%** in HK & Macau
- **Pharmaceuticals and Life Sciences**
- **6%** in mainland China
- **13%** in HK & Macau
- **Retail and Consumer**
- **42%** in mainland China
- **39%** in HK & Macau
- **Others**
Contacts

Hong Kong

John Donker  
Partner  
Forensic Services  
+852 2289 2411  
john.donker@hk.pwc.com

Megan Haas  
Partner  
Forensic Services  
+852 2289 1911  
megan.l.haas@hk.pwc.com

Chris Wilson  
Partner  
Forensic Services  
+852 2289 1993  
chris.p.wilson@hk.pwc.com

Shanghai

Antoinette Lau  
Partner  
Forensic Services  
+86 (21) 2323 5533  
antoinette.yy.lau@cn.pwc.com

Ramesh Moosa  
Partner  
Forensic Services  
+86 (21) 2323 8688  
ramesh.moosa@cn.pwc.com

Beijing

Brian McGinley  
Partner  
Forensic Services  
+86 (10) 6533 2171  
brian.mcginley@cn.pwc.com