Economic crime at work
Are we doing enough?

36%

More than one in three organizations expect to be victimized by economic crime

25%

One out of four respondents was asked to pay a bribe, more than regional or global counterparts

58%

More than half of respondents believe that local law enforcement agencies are not capable of combatting economic crime

pwc

www.pwc.com/ph/crimesurvey

Contents

Foreword

PwC conducts the Global Economic Crime Survey every two years, and 2016 marks the first time that results from the Philippines are published. The responses of Philippine companies have enriched the global survey, and have given us a snapshot of economic crime in the country. I feel that this survey is also very timely, given the new administration's focus on battling crime and corruption.

The results of the global survey show that economic crime is evolving globally, with its nature changing depending on the industry or region. Its financial impact has also been increasing while necessary preventive measures have been lagging.

Compared to the global average of 36%, only 20% of Philippine respondents reported experiencing economic crime over the past 24 months. However, the country is not exempt from this worrying trend. As borders are blurred for both businesses and criminals, economic crime is being perpetrated in different ways across emerging markets like ours. In fact, 36% of local survey respondents expect economic crime to be committed against them in the next 24 months.

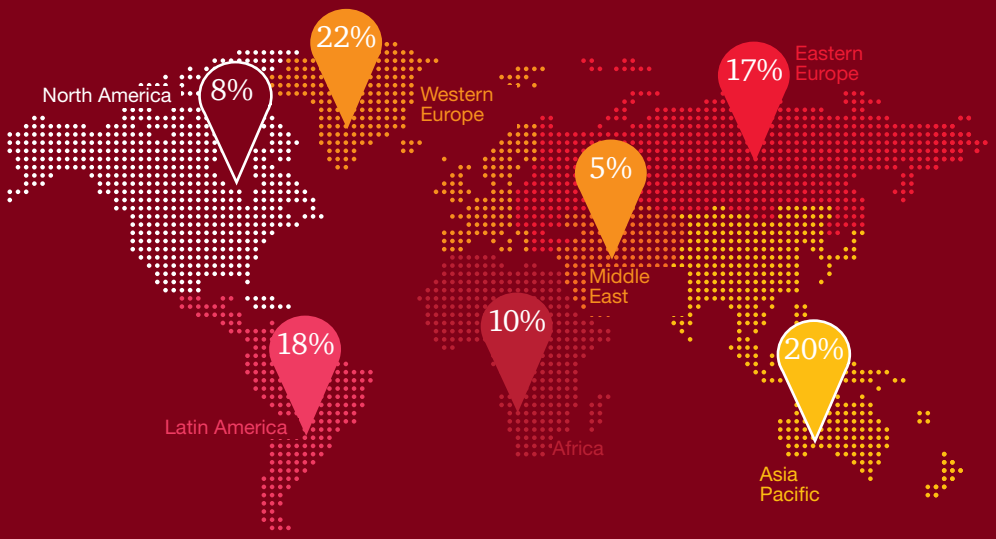
With an economy that is expected to grow at 6% per annum under the new administration, Philippine companies, in the pursuit of growth, might make insufficient token gestures to address the threats posed by economic crime.

An ever-changing global market is leading to an increased level of international cooperation in regulation and enforcement. Local organizations would do well to embrace the evolving challenges of economic crime by thinking globally and adopting international standards.

Benjamin B. Azada
Managing Principal, Consulting
Philippines

About the survey

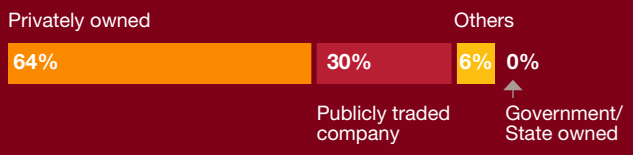
The 2016 Global Economic Crime Survey (GECS) received the inputs of 6,337 respondents from 115 countries, with 1,287 or roughly 20% of the respondents coming from the Asia Pacific region.



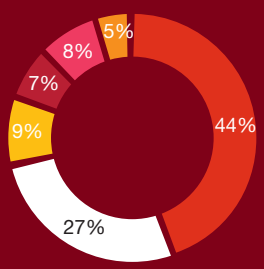
Global participation statistics

In the Philippines, 88 companies participated in the survey. These companies came from the following industries - manufacturing, financial services, business process outsourcing, automotive and general services. The respondents were split between those with 1,000 employees and below (50%) and those with more than 1,000 employees (49%). The majority of the organizations were privately-owned (64%).

Ownership structure



More than half of the respondents (56%) also had offices outside the Philippines.

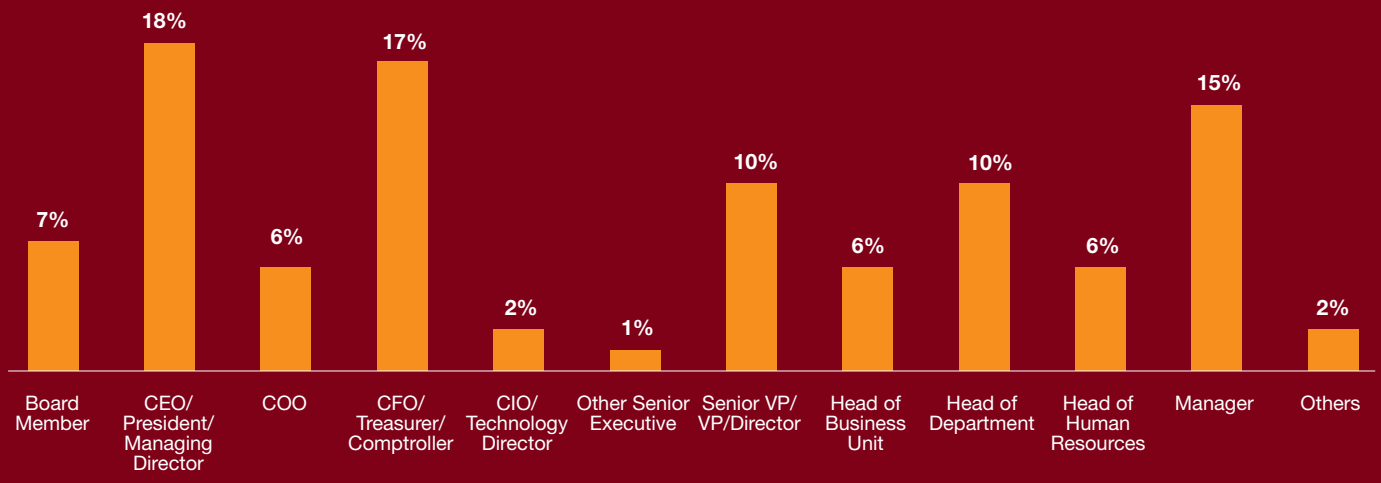


No. of countries with offices

- One only
- 2 - 10
- 11 - 25
- 26 - 50
- 51 - 100
- More than 100

The survey elicited the views of those with a key role in the organization. Half of the respondents were either a board member or a C-suite.

Roles of respondents




Global Economic Crime Survey 2016

Adjusting the Lens on Economic Crime

Preparation brings opportunity back into focus

36%

The Philippines' threat landscape

Prevalence

In the past 24 months, companies in the Philippines experienced a lower crime incidence than peers overseas. Economic crime rate was at 20%, compared with 30% in Asia Pacific and 36% globally.

Experienced economic crime (past 24 months)

Economic crime	Philippines	Asia Pacific	Global
Yes	20%	30%	36%
No	75%	58%	53%
Don't know	5%	12%	11%

Cybercrime rate at 17%, on the other hand, was also lower than 21% within the region and 26% globally.

Affected by cybercrime (past 24 months)

Economic crime	Philippines	Asia Pacific	Global
Yes	17%	21%	26%
No	72%	62%	56%
Don't know	11%	17%	18%

Of the 13 types of economic crime[1] listed, bribery and corruption remained a serious issue in the country, a reflection of the Philippines' consistently low ranking in Transparency International's Corruption Index.[2] Over the past 24 months, 25% of local companies were asked to pay a bribe while 17% said they lost an opportunity to a competitor due to bribery.

Bribery and corruption (past 24 months)

One out of four respondents was asked to pay a bribe, more than regional or global counterparts

1 Accounting Fraud, Asset Misappropriation, Bribery and Corruption, Competition/Anti-Trust Infringement, Cybercrime, Espionage, Human Resources Fraud, Insider Trading, Intellectual Property (IP) Infringement, Money Laundering, Mortgage Fraud, Procurement Fraud, and Tax Fraud.

2 Transparency International - https://www.transparency.org

Bribery became an even more serious issue considering the stance of top management as perceived by the organization's employees, as follows:

- did not consider bribery a legitimate practice (94%);
- took a public stand against corruption (91%); and
- resolutely backed corporate guidelines (87%).

However, only 76% of respondents believed that management would allow a business transaction to fail rather than resort to bribery, implying a disconnect between policy and action.

While bribery and corruption appears more common in the Philippines compared to other countries, it seems economic crime in general is less so. There are several reasons that could explain this:

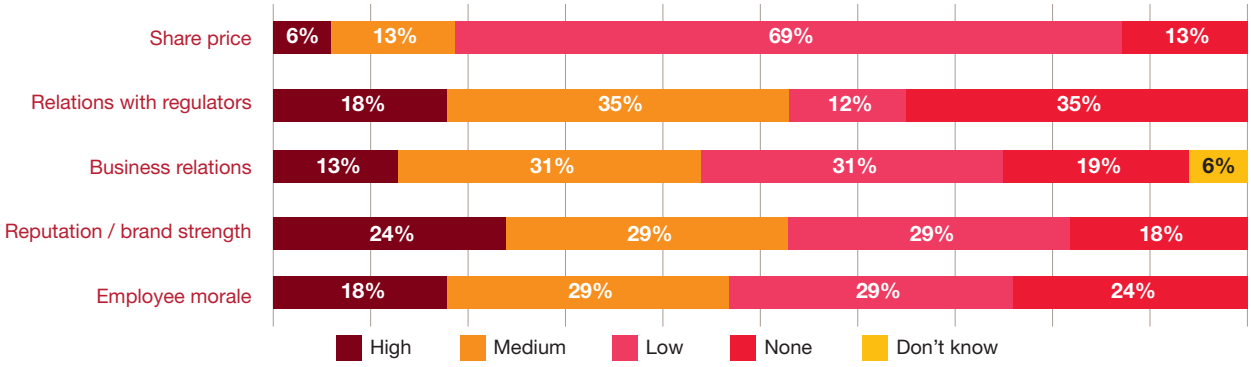
- Respondents might be hesitant to divulge sensitive and potentially embarrassing information about their companies, even if assured of confidentiality;
- Companies may have good control mechanisms in place; or
- Organizations may not be aware of economic and cybercrime being committed against them.

The last reason seems likely considering PwC findings that economic crime is changing significantly, but detection and controls programmes are not keeping up. For example, 72% of respondents claimed not to have been affected by cybercrime. However, these respondents could very well have been compromised without their knowledge due to the insidious nature of cybercrime. On the mobile platform alone, the Philippines ranked 7th most attacked country out of the 213 studied by a cybersecurity firm.[3] A close look at the organizations' preventive, detection, and response systems in place could give us a good indication if this low incidence is the result of good control mechanisms or non-detection.

Impact

While global financial losses related to economic crime have been increasing, the true cost of economic crime is difficult to quantify. Collateral damage is likely to have a bigger impact on long-term business performance. Philippine companies considered that economic crime committed against them in the past 24 months had the most impact on their Reputation/brand strength and Relations with regulators.

Impact of economic crime on business operations



3 http://business.inquirer.net/211611/ph-among-most-attacked-by-mobile-malware

Measures

Economic crime

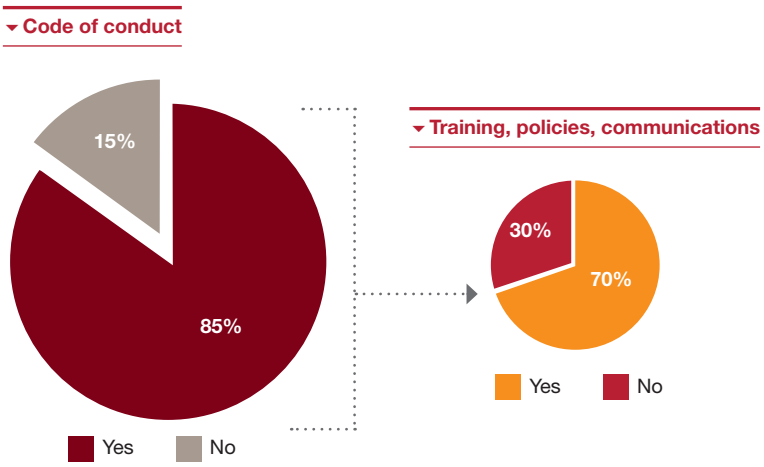
Fraud risk assessment

In the past 24 months, 61% of local organizations performed a fraud risk assessment at least once or periodically. However, there were more local organizations (26%) that had not conducted a fraud risk assessment in the same period compared to regional (23%) and global (22%) counterparts.

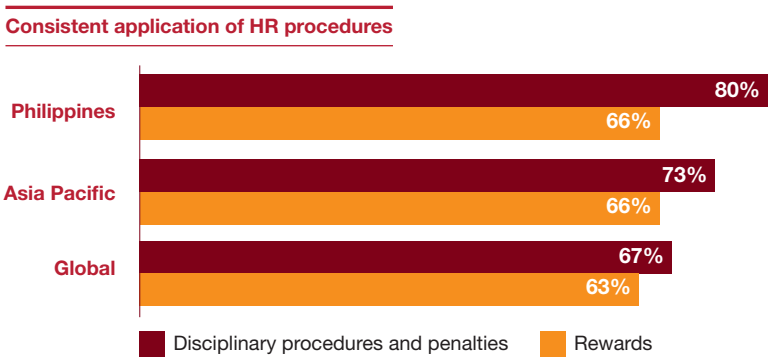
Ethics and compliance program

The majority of local organizations had a formal business ethics and compliance program (78%), with a Chief Compliance Officer responsible for the program (44%). Organizations were most likely to use Internal audit (83%), Management reporting (55%) and External Audit (44%) to ensure the program's effectiveness.

While 85% of local organizations had a Code of Conduct that covered key risk/policy areas and set out the organizational values and the behaviour expected of all in the organization, only 70% regularly provided training, supporting policies, and communications on the Code.



The Philippines followed regional and global trends (roughly 80%) of companies with Human Resources (HR) procedures—such as objectives, promotion, reward, recognition, and disciplinary procedures—that gave importance to ethical business conduct. Similarly, more companies consistently applied negative reinforcement (disciplinary procedures and penalties) than positive ones (rewards). The disparity between the two, however, was wider in the Philippines.



Fraud risk assessment plays a crucial role in developing and maintaining effective fraud risk management programs and controls. Thus, an organization needs to periodically assess its fraud risk exposure to identify specific potential schemes and events that the organization needs to mitigate.

Ethics and compliance program

Organizations must have a robust Ethics and Compliance Program embedded throughout their operations. The program's focus must be extended to:

1. include people and culture;
2. reflect the company specific risk and organizational profile; and
3. be aligned with the organization's business strategy.

Two reasons could account for this preference for negative reinforcement.

- The majority of local companies have a legalistic approach to human resources, following the provisions of a Philippine Labor Code that lean towards penalties instead of rewards. A developmental approach to HR is less common.
- The relationship between management and labor remains traditional, meaning adversarial.

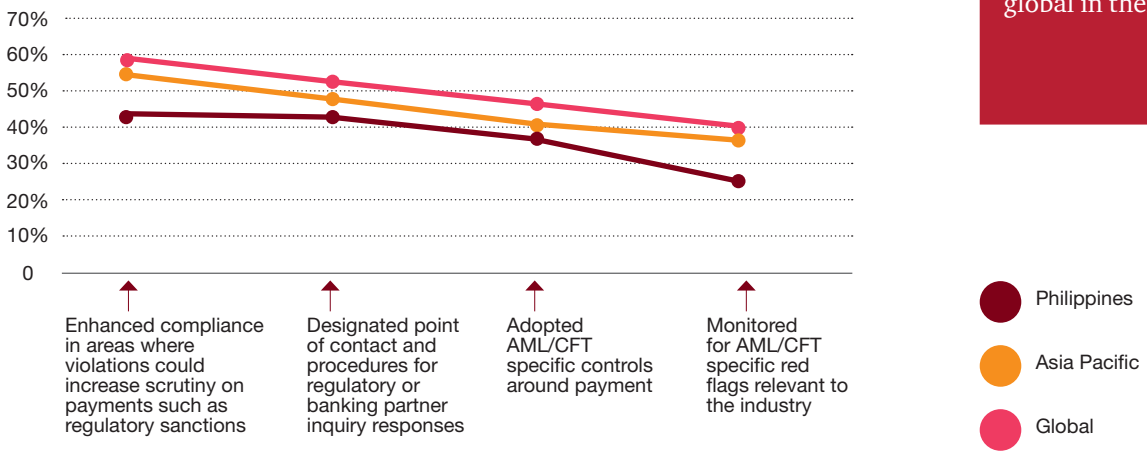
Anti-Money Laundering – Combating the Financing of Terrorism (AML/CFT)

In recent months, the country made headlines when a local bank was allegedly used by criminals to launder millions of dollars stolen from a South Asian bank. This highlights the need for a robust Ethics and Compliance Framework at the enterprise level. While the country has an anti-money laundering law (R.A. 10365) and local AML rules and regulations (BSP[4] Circular 2011-706) and risk rating system (BSP M-2012-017), clearly more needs to be done.

Based on the GEC survey, local companies generally lagged behind their regional and global counterparts in implementing AML/CFT measures.

Less than half of respondents (44%) enhanced compliance in areas where violations could increase scrutiny on payments such as regulatory sanctions and had designated point of contact and procedures for regulatory or banking partner inquiry responses. Only a quarter monitored for AML/CFT specific red flags relevant to the industry while a third (38%) adopted AML/CFT specific controls around payment.

AML/CFT Measures (Past 24 months)



Through the years, the global community has enhanced its anti-money laundering controls in order to combat the financing of terrorism by protecting the integrity and stability of the financial system and cutting off resources being used by terrorists, thus making it more difficult for terrorists to profit from their criminal activities.

Since money laundering is no longer confined within banks, it now expands across other industry sectors, especially with the introduction of many alternative payment mechanisms in the market. Regulations are more frequent, more stringent and more global in their approach.

Local companies did slightly better when it came to limiting their exposure to trade based money laundering activity, with the same number of respondents (48%) establishing controls around payments to/from third parties as their regional counterparts. At 27%, more Philippine organizations than regional and global ones conducted real time monitoring of adverse information related to all business partners.

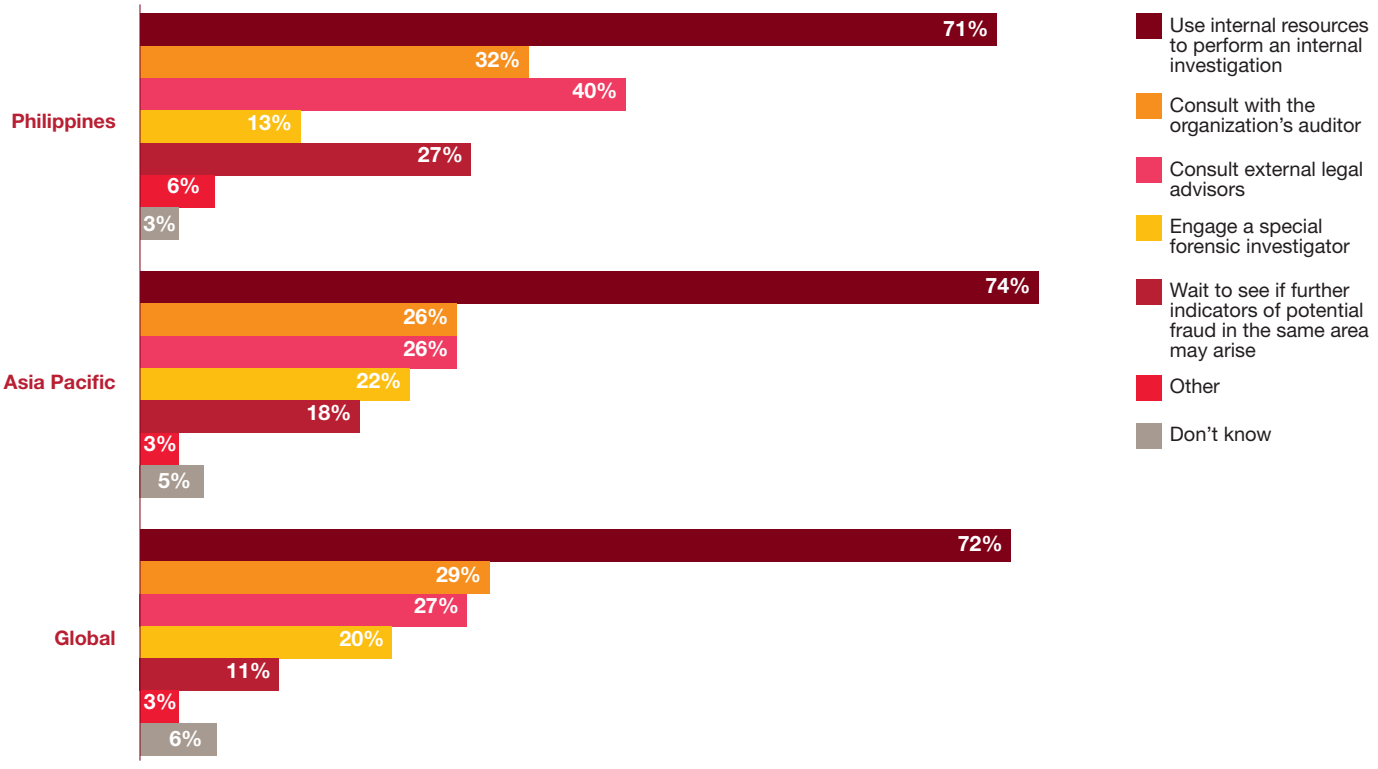
4 *Bangko Sentral ng Pilipinas* or Central Bank of the Philippines

Philippine companies however fell short in other measures. Only 20% of respondents conducted third party due diligence at start of relationship with all business partners (clients, agents, customers) to include ownership structure, nature of business, expected activity, etc. compared to the Asia Pacific average of 30%. At 33%, more local respondents compared to 31% regional companies did not consider their business to be at risk and thus took no measures specifically to limit exposure to trade based money laundering activity. 6% of respondents took no measure at all despite acknowledging that the business could be at risk.

First response

In the face of potential fraud, the top three actions of Philippine companies were to use internal resources to perform an internal investigation (71%), contact external legal advisors (40%), and consult with the organization's auditor (32%). These actions were consistent with regional and global company practice. Other territories however were more likely to engage a special forensic investigator compared to the 13% of local companies that were likely to do so. Philippine companies also seemed to be more passive, with 27% content to wait to see if further indicators of potential fraud in the same area may arise, compared to the 18% regional average and even lower 11% global average.

Actions likely to be taken when an incident of potential fraud is identified



From these statistics, it appears that Philippine companies are not yet aware of the value of employing specialized forensics practitioners to investigate economic crime.

Cybercrime

While security experts considered the Philippines as increasingly exposed to cyber threats (33rd out of 233 countries),[5] local companies seemed to think otherwise. Only 17% of respondents said they had been victims of cybercrime. This perception could be the reason they took the threat of cybercrime less seriously.

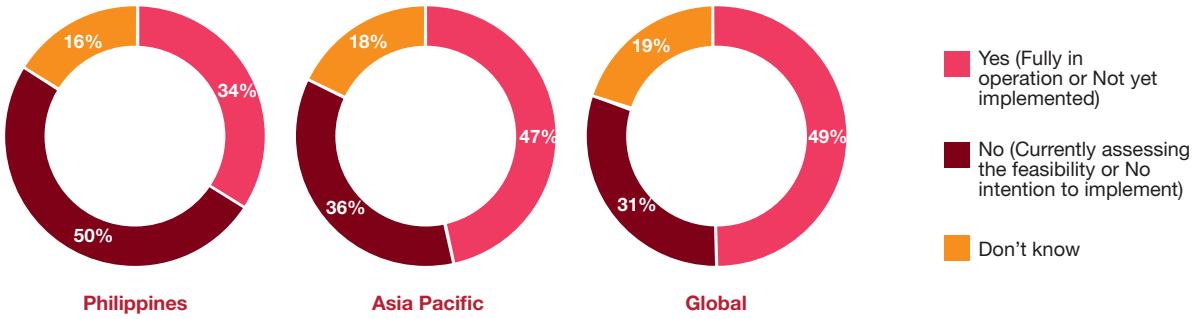
Engaging leadership in dealing with cyber incidents is critical. However, board members in only 36% of the respondent companies asked for information on their organizations' state of cyber-readiness. Almost half (48%) did not ask or consider asking for such information.

Frequency Board members request information on organization cyber-readiness

Economic crime	Philippines	Asia Pacific	Global
Monthly	6%	6%	8%
Quarterly	16%	18%	19%
Annually	14%	15%	16%
Board members do not request this information	31%	24%	19%
Board members have not considered the need for this information	17%	11%	10%
Other (please specify)	3%	3%	4%
Don't know	13%	23%	25%

Only a third (34%) of local organizations also had an incident response plan compared to 47% in the region and 49% globally.

Incident response plan to deal with cyber attacks



5 http://www.rappler.com/newsbreak/in-depth/130883-state-cybersecurity-philippines

Government

The Philippines has a number of laws addressing cyber crimes such as the 2012 Cybercrime Prevention Act (R.A. 10175). However, these laws deal mainly with the aftermath of the cyber crime and few Philippine companies (14%) expressed confidence in the ability of local law enforcement agencies to investigate cybercrime. The Department of Information and Communications Technology was recently created (R.A. 10844)[6] to deal with ICT matters, including cybercrime. It remains to be seen, however, whether the Department will be able to effectively combat cybercrime and increase the confidence of local organizations.

If they were not convinced of local agencies' ability to investigate cybercrime, Philippine companies expressed even less confidence (5%) when it came to economic crime in general, with the Philippines coming in 4th among countries that did not believe local agencies had the resources to combat economic crime.

Top 10 countries that believe their local law enforcement agencies are not adequately resourced to combat economic crime

1	Kenya	79%
2	South Africa	70%
3	Turkey	60%
4	**Philippines**	**58%**
5	Bulgaria	58%
6	Poland	58%
7	Ukraine	57%
8	Mexico	56%
9	Zambia	55%
10	Nigeria	54%

More than half of respondents believe that local law enforcement agencies are not capable of combatting economic crime

The implications of such low levels of confidence in law enforcement are obvious. When it comes to preventing and responding to economic crime, companies have to do it themselves. And there is no time like the present considering that companies expect more economic crime to be committed against them in the next 24 months.

6 http://www.philstar.com/headlines/2016/05/24/1586363/p-noy-signs-law-creating-ict-dept

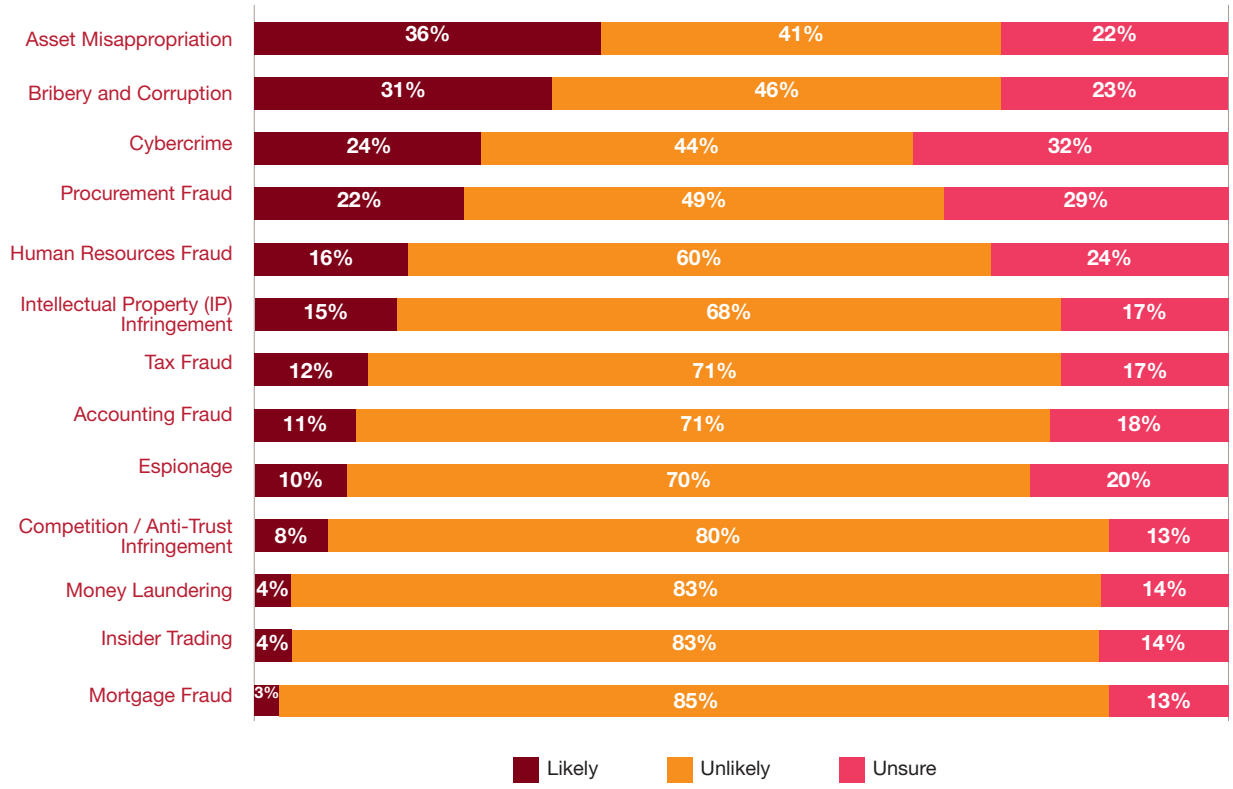
Emerging threats in the Philippines

Major threats

Despite reporting a low incidence of economic crime in the past 24 months, Philippine companies were less optimistic about the near future. Similar to other territories, 36% of companies in the Philippines thought it likely that Asset Misappropriation would be committed against them in the next 24 months. Bribery and corruption claimed the second spot at 31% while cybercrime made it to the top 3 at 24%. Money laundering came a distant 11th place, with only 4% of respondents considering this crime likely to occur.

More than one in three organizations expect to be victimized by economic crime

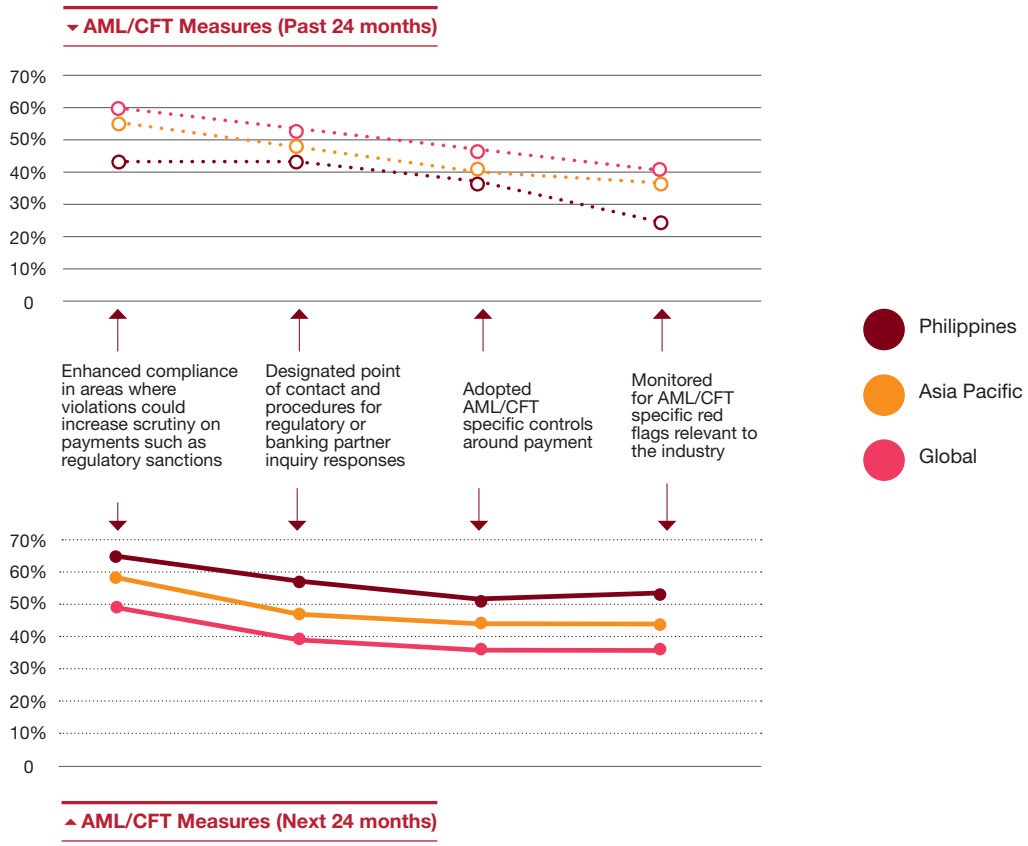
Likelihood of economic crime (Next 24 months)



Course of action

In the face of increased threats, only 9% of companies in the country planned to significantly increase their compliance program and resource spend, 36% intended to see some increase, while the majority (54%) intended to keep the same level of spend.

However, when it came to Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT), it appears that local companies intended to do much better. Philippine companies trailed behind regional and global counterparts in the implementation of such measures in the past 24 months, but more of them planned to implement AML/CFT measures in the next 24 months. This despite money laundering only placing 11th among expected economic crimes.



Over the years, the Global Economic Crime Survey has shown that as market conditions evolve, so does the threat landscape that accompanies them. Regulations and standards will become increasingly complex and demand even greater public accountability as economic crime continues to plague businesses. It is thus necessary that an organization's approach to ethics and compliance be risk-based and for risks and programs to be regularly re-assessed.

As more and more Philippine organizations strategically aim to participate in the global marketplace, their exposure to economic crime increases accordingly. Organizations should take this opportunity to look ahead to anticipate and manage economic crime while thinking business expansion globally. At this phase, strategic business growth should be carefully balanced with enterprise risk management by mitigating operating and fraud risks. Today's fast paced global marketplace requires nothing less than a proactive approach in dealing with economic crime risks.

Contacts

Benjamin B. Azada
Managing Principal, Consulting
Philippines
T: +63 (2) 459 3011
benjamin.azada@ph.pwc.com
https://ph.linkedin.com/in/benjazada

Roberto C. Bassig
Director, Technology and Cybersecurity
Philippines
T: +63 (2) 845 2728 ext. 3143
roberto.c.bassig@ph.pwc.com
http://linkedin.com/in/roberto-bassig-68778714

Aurelio Mari G. Gueco, CFE
Senior Manager, Risk and Forensics
Philippines
T: +63 (2) 845 2728 ext. 3231
aurelio.mari.gueco@ph.pwc.com
https://ph.linkedin.com/in/religueco