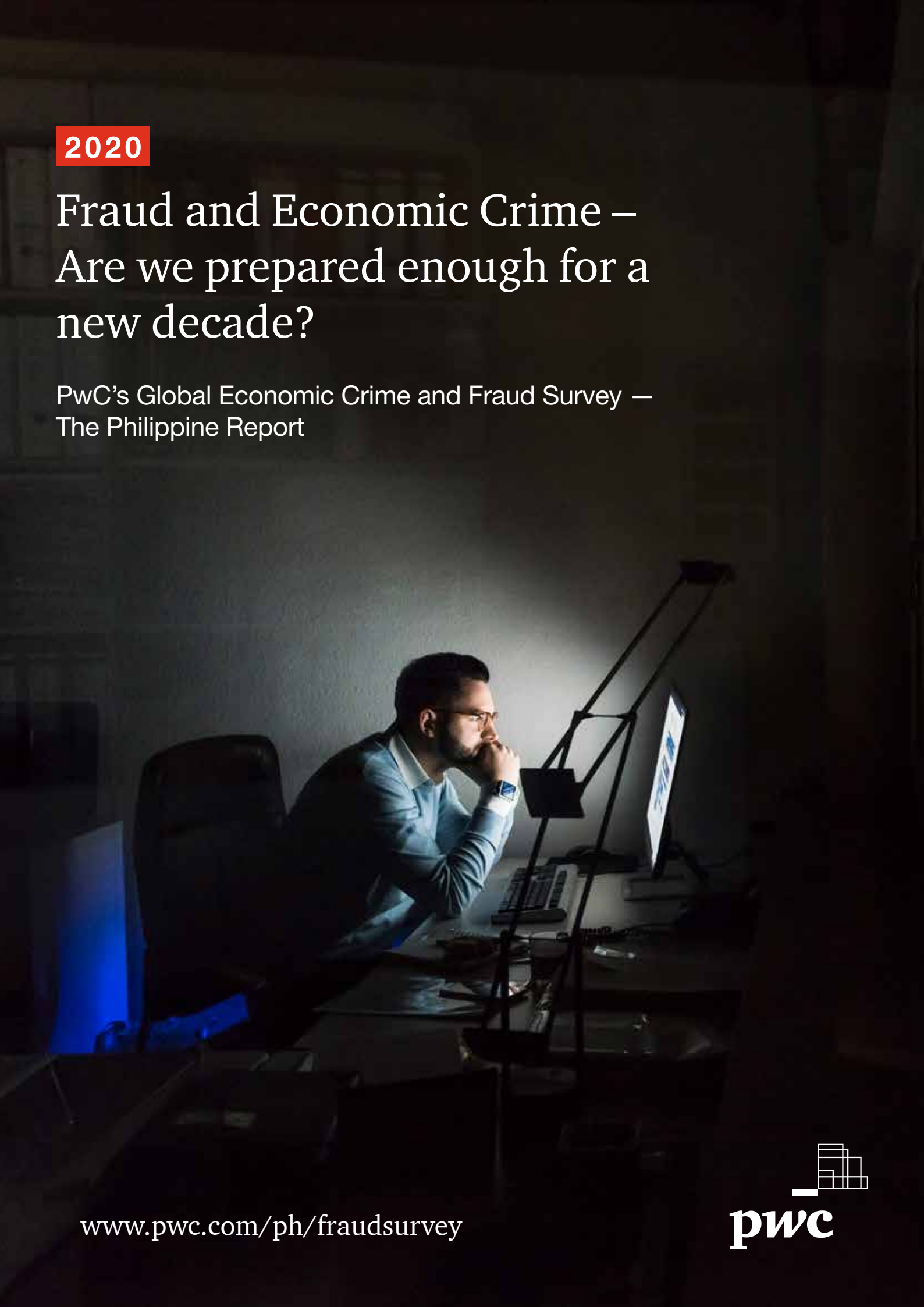
2020

Fraud and Economic Crime – Are we prepared enough for a new decade?

PwC's Global Economic Crime and Fraud Survey — The Philippine Report



www.pwc.com/ph/fraudsurvey

pwc

Contents

Foreword

Over the last decade, we have seen our country grow from what was once the Sick Man of Asia to an Asian tiger cub, with one of the most stable and vibrant economies in Southeast Asia in recent history.

Based on the forecasts of economic experts, the Philippines is poised to continue experiencing such growth, eventually growing to become among one of the top 20 economies in the world after another two decades. This indeed paints a very promising picture of the bright future that we are leaving for the next generation of Filipinos!

However, bright lights often cast dark shadows which, when left unattended, can sometimes grow to eclipse the bright lights. This is exactly the place where we find ourselves, as can be seen with an ever-increasing number of economic crimes (such as fraud and corruption) committed in the Philippines. Beyond quantity, advancements in technology have also allowed fraudsters to grow the scale and complexity in which they perpetrate these economic crimes. There is also some variation in terms of where these activities are being done as well as who is doing them. This much is apparent from local news reports, the results of this survey, as well as in the findings of reports published by other global experts such as Transparency International, World Economic Forum and the World Bank.

Awareness of economic crimes is indeed increasing, but the question is–are we doing enough to meet the demands of the new decade? With the continued clamor for increased transparency, higher standards of trust, and even greater accountability among key stakeholders such as shareholders, investors, regulators and the general public, it is clear that there's a lot more work to be done.

In this sense, it is very important to highlight the importance of integrity and technology.

One could have the best tools on hand, but all of these would be rendered useless if their users do not act with integrity. Integrity is a behavior that needs to remain, regardless of the changes in the ways of doing things. This is a mantra that we should always keep in mind–from how we run our businesses, to how the private sector collaborates with the government to make the Philippines a better place, to how big businesses find ways to help small and medium enterprises grow, and even to how we educate the next generation of Filipinos.

For the modern-day organization, integrity is best exemplified by the actions of the board of directors and the management team–the tone at the top. In an ideal corporate governance set-up, the people at the top need to be able to convey and exemplify how one acts with integrity, as well as provide oversight on whether or not those on the ground tend are able to mirror such behavior. This is precisely why integrity is a highly prized quality for the members of the board and management to have.

The role of technology in fighting fraud cannot also be undermined. Investments in good technology greatly help in detecting and stopping fraud in their tracks, safeguarding businesses from the often large, adverse impacts of fraud and even serving as a deterrent against future attempts by fraudsters. Despite the large initial outlay, given the scale and complexity at which economic crimes and fraud are growing, these investments are sure to pay themselves back by making the process of fighting against fraud more efficient and effective.

Indeed, if we are to meet the challenges of tomorrow and shine a light on the shadow cast by economic crimes, we must prepare for them in the here and now.

Atty. Alexander B. Cabrera
Chairman & Senior Partner,
PwC Philippines
Chairman, Integrity Initiative

On behalf of the team, I am privileged to present the third Philippine report of PwC's biennial Global Economic Crime and Fraud Survey.

Firstly, we would like to thank all the Philippine companies who have responded to the survey. It is with your participation and willingness to share insights on economic crime and fraud that this report has been made possible.

It has been a quick two years since we presented the results of the second Philippine report, and we have seen quite a number of developments in the fight against economic crimes, both locally and abroad. Still, the incidence of fraud at organizations continues to remain high, with at least 42% of Philippine respondents reporting having encountered economic crime and fraud over the last two years. It is also apparent that organizations are continuing to raise awareness within their organizations of what economic crimes are, including how to fight them.

With the turn of the decade, it is clear that there's more to come in the next phase of the country's growth story. The Philippines is expected to continue to gain steam in spite of rapid shifts in technology, higher competition in global trade, and greater complexity in regulatory regimes. This is precisely why the fight against economic crime and fraud is more important than ever.

For one, there has been a great uptick in the number of technology-enabled economic crimes, with the number of cybercrime investigations performed by local authorities increasing exponentially over the past few years. An ever-competitive business landscape also means that the pressure is on, with organizational actors urged to achieve greater business results from one year to the next, leading some to stray from the path of integrity. If we don't proactively find the right governance needed to address the threats and leave them unchecked, we might end up undoing the good progress that we have made over the last decade.

Still, the future looks promising. Regulators both local and overseas are also accelerating their concerted efforts to stop economic crimes and fraud in their tracks, by not only increasing regulatory scrutiny on the capability of organizations to fight them, but also by prescribing base and practicable usable guidelines and working more closely with the private sector to help struggling organizations keep up.

Businesses, on the other hand, are further preparing themselves to face the challenge of economic crimes and fraud in the new decade by enhancing their ability to manage their consequences. Efforts to strengthen corporate governance, risk management, internal controls and transparency are also evident in the last two years, judging by the increased collaboration between the private and public sectors. The challenge for the new decade is keeping such efforts consistently going, as well as finding a way to accelerate and innovate in order to meet and keep up with the pace of change in the economic crime and fraud landscape. As comrades in fighting against fraud, let us keep the conversation going and help one another!

Roberto C. Bassig
Risk & Technology Consulting
Partner, PwC Philippines

Executive summary

Latest economic reports by the Philippine Statistics Authority peg the 2019 Philippine GDP growth rate at 5.9% year-on-year. While this is the slowest growth rate for the Philippines since 2011, such growth is still among the highest in the Southeast Asian region, as well as globally.

With this growth, economic crime and fraud in the Philippines also continue to increase, hitting at least one out of two business respondents who reported having experienced economic crime and fraud in the past 24 months, with losses ranging from $5m to $50m. Among those who reported in the affirmative, the majority of respondents reported having experienced an average of five (5) fraud incidents over the last 24 months, while 10% specifically reported having experienced at least six to more than ten incidents of fraud during the same survey period.

In PwC's 2020 Global Economic Crime and Fraud Survey – The Philippine Report, asset misappropriation fraud continues to be the most disruptive to Philippine businesses, with at least 26% or one out of four businesses having experienced it since 2018. Truly, this type of fraudulent scheme has always been an especially unyielding threat even among businesses around the globe. And this poses an imminent threat to the continued resilience of a strong economy such as that of the Philippines.

Bribery and corruption is another obstinate threat, the second most disruptive economic crime in the Philippines. This year's results reveal that this particular type of fraud picked up again over the last 24 months, moving up by three notches from fifth last year to 21% in 2020, from 18% in 2018, and 25% in 2016. Another 14% of respondents (from 12% in 2018 and 17% in 2016) have also alleged that they have lost a business opportunity from a competitor who paid bribes. These outcomes mirror the results of the annual Corruption Perceptions Index by Transparency International, which saw the Philippines' rank drop from 99th to 113th. This is concerning as businesses operating in the Philippines may be more likely to contemplate paying bribes as a feasible option to take in order to win business.

Our study also revealed that external perpetrators of economic crime and fraud may have contributed significantly to the staggering loss of $5m to $50m mentioned above. Over the course of the last 24 months, the number of fraud incidents that involve external actors (with or without help from internal actors) have increased to 50% as compared to 20% in 2018.

There are a few reasons that may point to why this was the case. For one, investment and adoption of technologies to combat economic crimes generally continue to be rather low among businesses operating in the Philippines. Two, there are provisions in Philippine laws and regulations such as the Bank Secrecy Act and the Anti-Money Laundering Act that potentially hamper the ability of investigators to collect the full evidence needed to prosecute a fraudster. Furthermore, despite the tightening of some laws and regulations, the ability of government regulators and organizational oversight functions to scrutinize compliance remains inadequate and spotty due to cost constraints.

More often than not, organizations in the Philippines may have been forced to learn the importance and value of investments in fraud-fighting initiatives after having had to deal with economic crime and fraud within their respective organizations. Aside from their impact to the bottom line, economic crimes and fraud have created frustration, sleepless anxiety and a stressful work environment for at least one out of three respondents. Not to mention, these economic crimes and fraud may have a long-term reputational impact, which may result in higher regulatory scrutiny and monetary penalties in the future.

Our survey results reveal that fraud committed by internal actors has had a big drop to 38% from 67% in 2018. Twenty-six percent (26%) of respondents also have plans to increase the amount of funding they dedicate to combating fraud over the next 24 months while 35% intend to maintain such funds at their current levels. This is a reflection of how Philippine businesses have been serious in stepping up their corporate governance. Businesses have embraced common best practices to fully address the enterprise-wide risk of economic crime and fraud, such as: 1) significant improvements in internal and cyber controls, 2) enhancement of policies and procedures, 3) investment on the right integrated/automated tools and applications, 4) investment on hiring and/or training the right people to conduct and monitor a robust anti-fraud framework, and 5) implementation of an effective whistleblowing network to capture reports on any anomalous schemes.

Threats and gaps

How ready are you?

Fraud and economic crime rates remain at at record highs, impacting more companies in more diverse ways than ever before. With this in mind, businesses should be asking: “Are we assessing threats well enough...or are gaps leaving us dangerously exposed?”

With fraud a greater – and more costly – threat than ever over the last 20 years, it’s essential to assess the company’s readiness to deploy effective fraud-fighting measures, and act quickly once economic crime is uncovered.

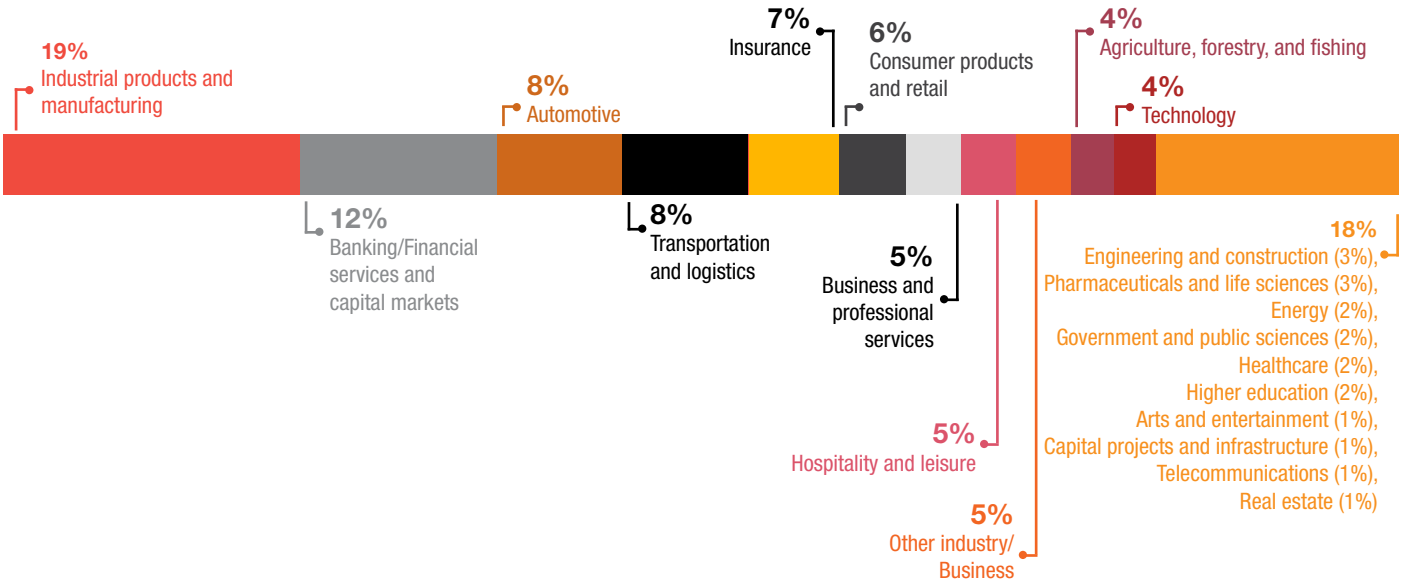
Source: PwC’s 2020 Global Economic Crime and Fraud Survey

About the survey

Over the last 20 years since its inception in 2001, PwC's Global Economic Crime and Fraud Survey (GECS) has been one of the premier thought leadership publications on economic crime – globally! More than 5,000 respondents across 99 countries (including 101 from the Philippines) have shared their experience of economic crime and fraud over the past 24 months, incurring a staggering US$42bn in losses.

The aim of GECS is to assess corporate attitudes towards fraud and economic crime in the current economic environment and how these, in turn, have impacted organizational business ethics and compliance programs. GECS also looks into how what types of fraud are most common among business organizations, how they are affecting internal stakeholders and the corresponding response to fraud.

Industries where organizations mainly operate



Profile of the Philippines' respondents

50% of respondents are locally established companies while the other half are MNCs that have operating offices in the Philippines.

Further, **40%** of respondents belong to large organizations that have between 1,001 to 5,000 employees and annual revenue turnover of about $10m to $50m.

62% are privately owned and **22%** are publicly traded companies.

42% are having extensive insights and/or high level knowledge about the fraud that happened over the last **24** months.

Respondents are mostly C-Suites from the Executive, Finance and Internal Audit Departments.

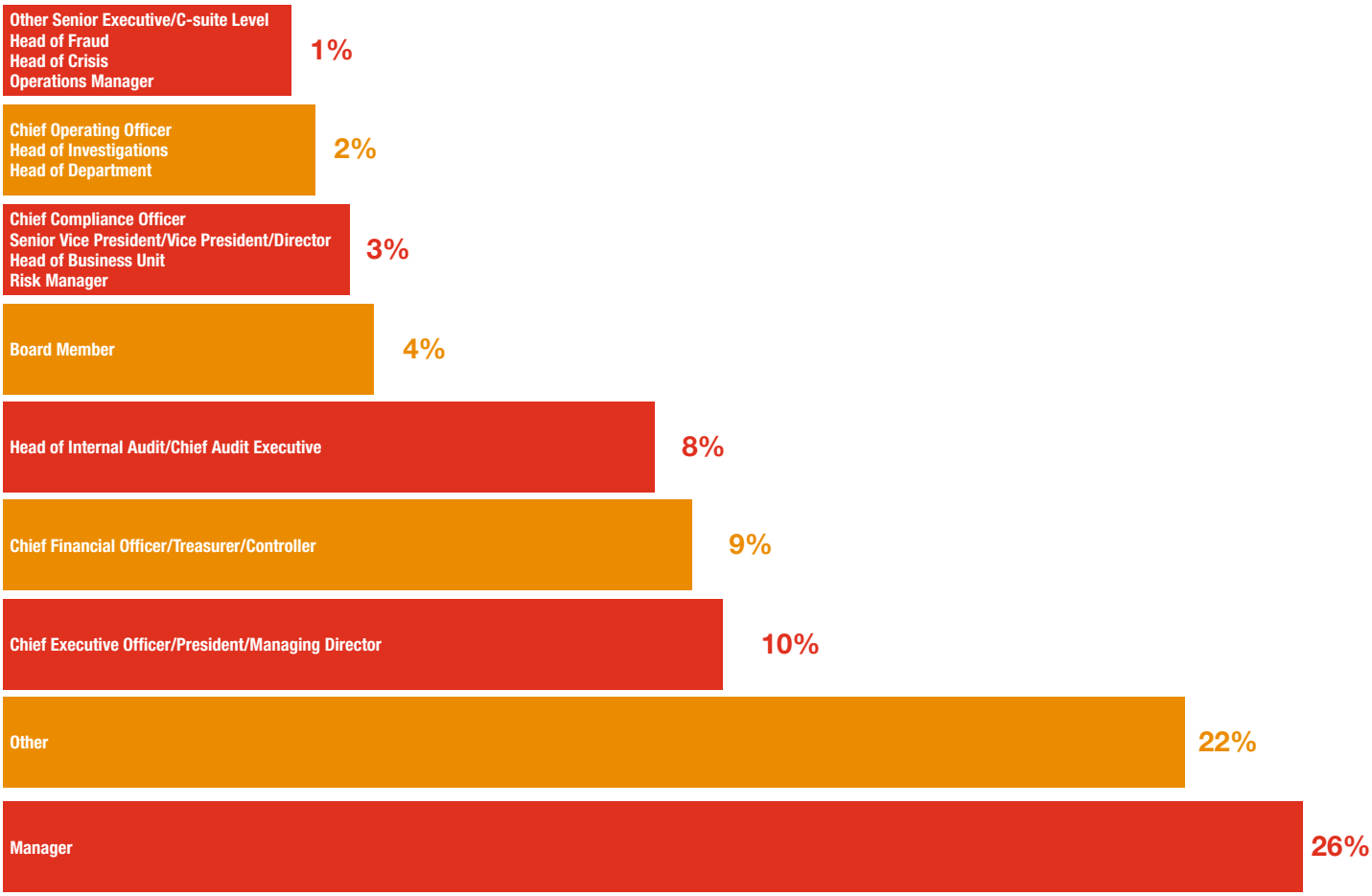
4 out of 10 respondents reported that they have experienced economic crime and fraud over the last 24 months...

43% of the above respondents have experienced **two to five incidents of fraud,** and...

10% had experienced over **six to 12 incidents of fraud!**

Only **4%** of respondents maintain specialized employees whose primary function is to conduct investigations on fraud and financial crimes within the organization.

Respondents' job title/role



Learnings at the end of a decade

As we enter the new decade with new challenges ahead, let us have a glimpse on how fraud incidents have impacted Philippine business.

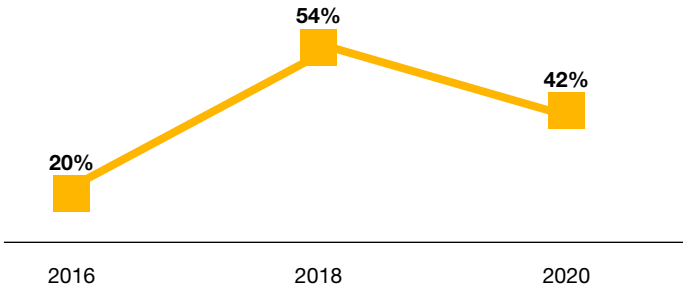
How much are we being defrauded?

Fraud incidents in the Philippines have not diminished, and in fact may have been on the rise over the past six years[1].

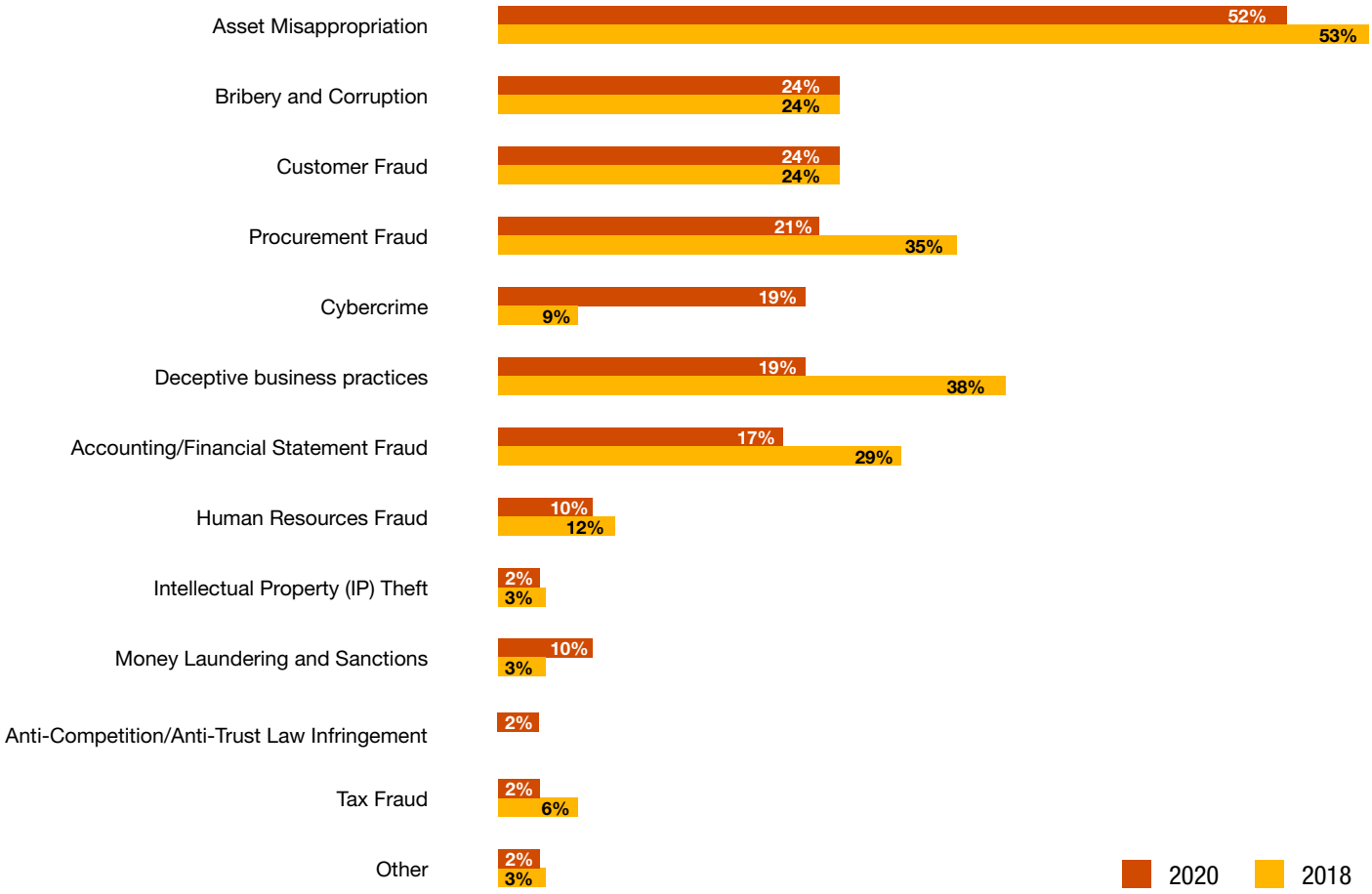
Although there is a decline in percentage terms, it is useful to note that there were only 63 respondents in 2018 versus 101 this year. This means an increase in the number of fraud incidents from 2018 at 32, to 2020 with 42.

Areas of asset misappropriation, customer fraud and bribery have been the most prevalent in the local scene.

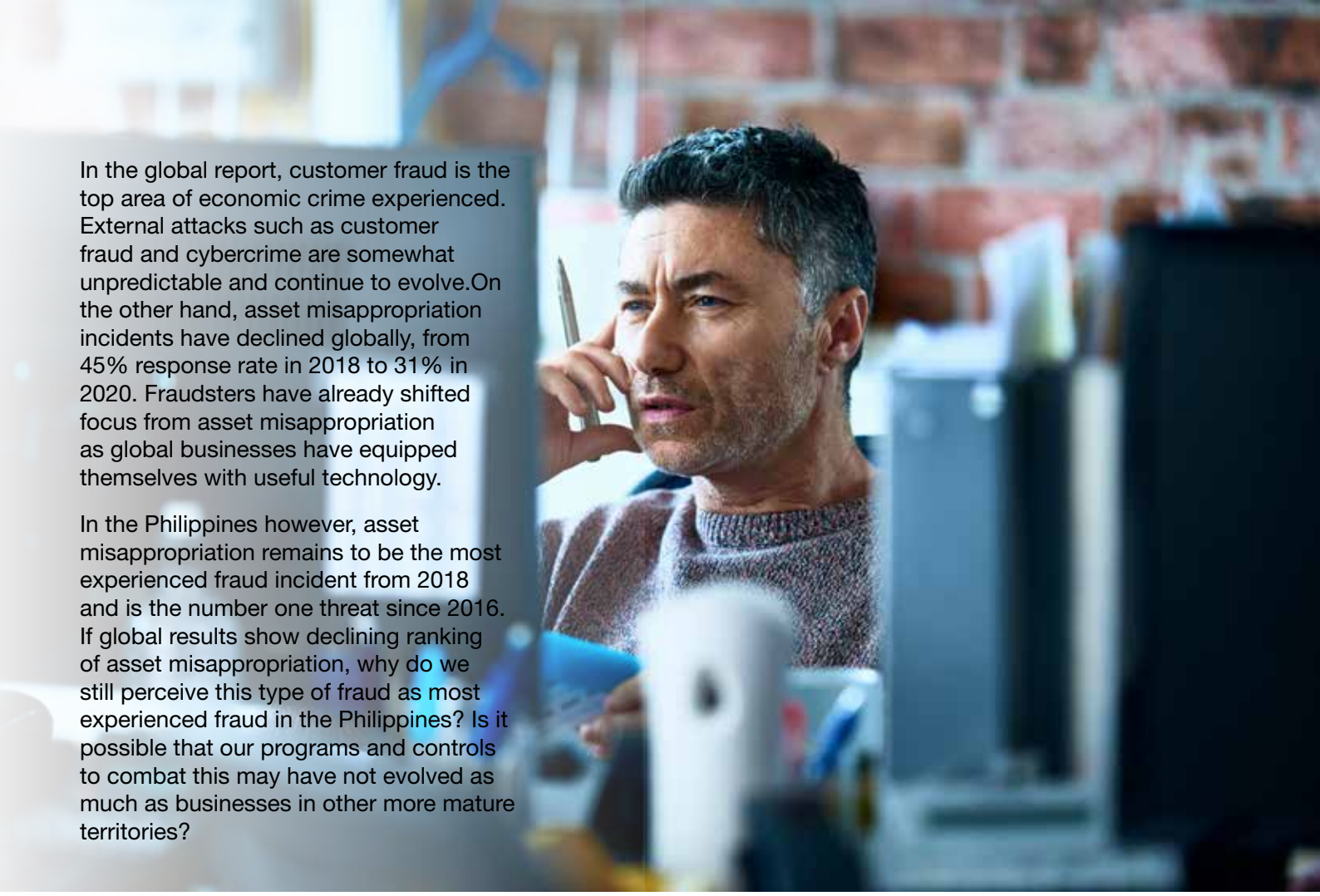
Fraud incidents in the Philippines



Economic crimes in the Philippines



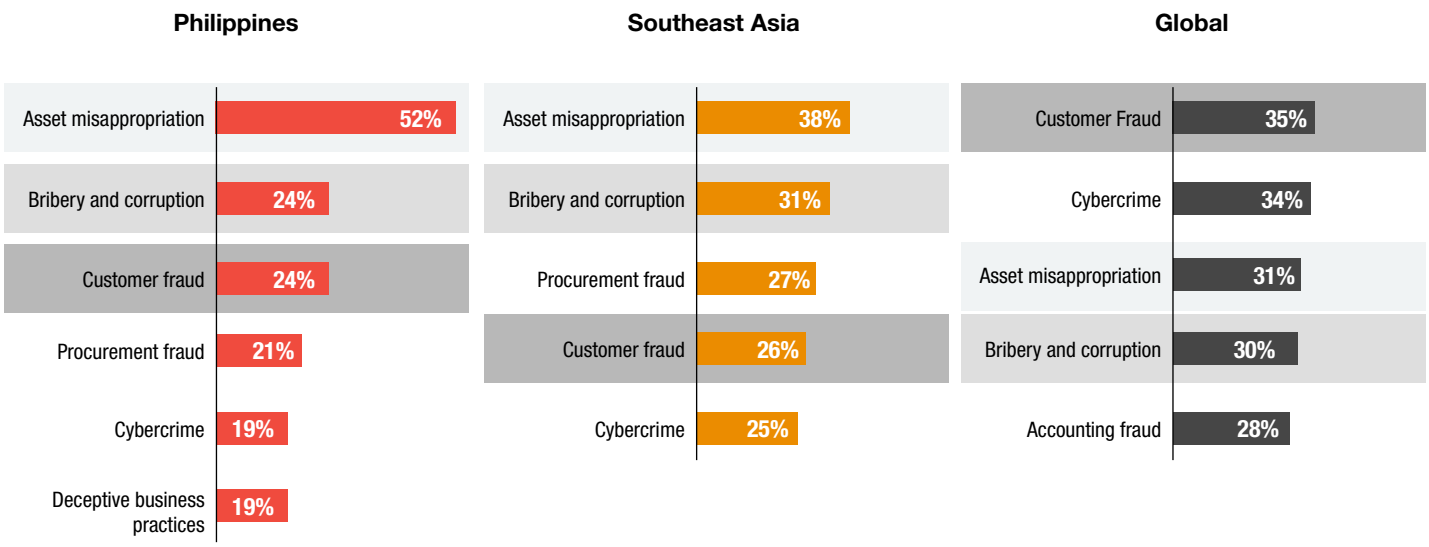
1 Comparative figures are with 2016 and 2018 survey results



In the global report, customer fraud is the top area of economic crime experienced. External attacks such as customer fraud and cybercrime are somewhat unpredictable and continue to evolve.On the other hand, asset misappropriation incidents have declined globally, from 45% response rate in 2018 to 31% in 2020. Fraudsters have already shifted focus from asset misappropriation as global businesses have equipped themselves with useful technology.

In the Philippines however, asset misappropriation remains to be the most experienced fraud incident from 2018 and is the number one threat since 2016. If global results show declining ranking of asset misappropriation, why do we still perceive this type of fraud as most experienced fraud in the Philippines? Is it possible that our programs and controls to combat this may have not evolved as much as businesses in other more mature territories?

Top five types of fraud, corruption and economic crime experienced in the past 24 months



A spike in bribery and corruption

Incidents of bribery did not diminish in the Philippines from previous years. In fact, in the Transparency International Index for 2019, the Philippines landed at 113/180 (from 99/180 in 2018), while Thailand ranked 101/180, and Vietnam ranked 96/180.[2]

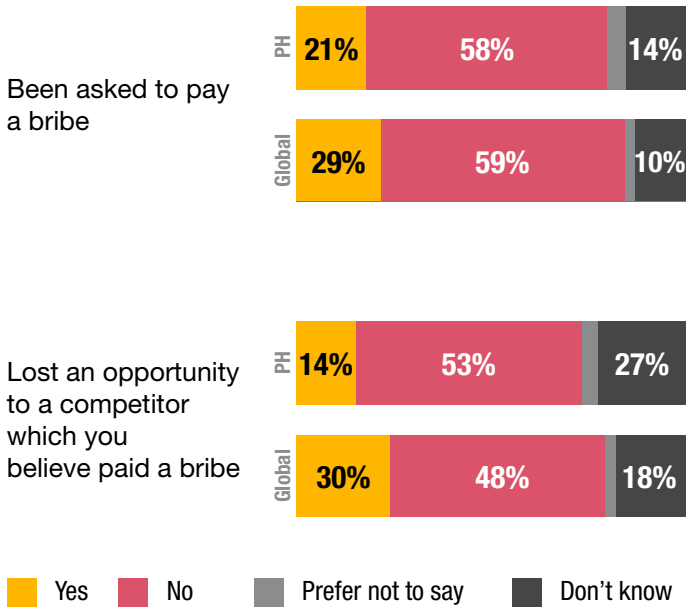
In 2020, 21% of respondents said they were asked to pay a bribe while 14% of respondents said they lost an opportunity to a competitor who they believed paid a bribe. Although this is lower compared to global results, the experience of Philippine businesses in bribery has been fluctuating between 2018 and 2016 results.

Cybercrime may be the only crime of tomorrow

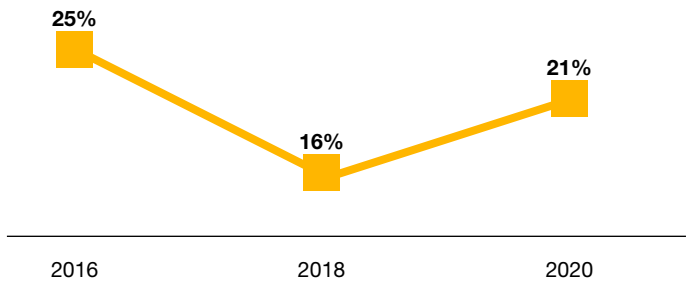
Cybercrime continues to emerge as technology evolves. New threats and schemes are being developed by perpetrators coming from usual cyber attacks such as email spoofing and phishing, online scams, and identity theft. We observed recently that fraud schemes such as asset misappropriation, procurement fraud and accounting-related fraud are being committed through a cyber attack where perpetrators spend years observing business behaviors to find the perfect opportunity and time to facilitate wire transfers, payments, goods delivery, fake purchases, etc.

The Philippine National Police – Anti Cybercrime Group released statistics of cybercrimes investigated for a period of six years. Number of investigations made on different types of cybercrime catapulted as high as 510 times from 2013 to the first half of 2019[3]. Cybercrime also continues to be a growing threat to global businesses, according to the 22nd PwC Annual Global CEO Survey. Cyber threat is the fifth top threat that executives in 90 territories around the world are extremely concerned about. Included in the top ten threats is also the speed of technological change, which also directly enables cyber related crimes.

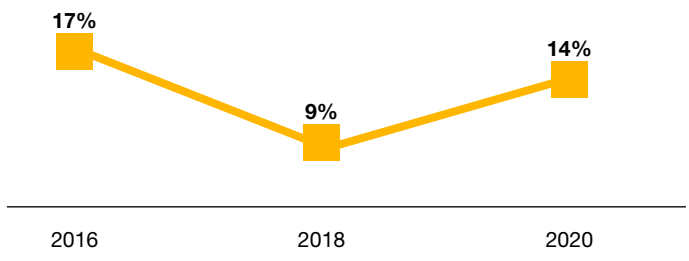
In the last 24 months, has your organization:



Has your organization been asked to pay a bribe?



They lost an opportunity to a competitor which you believed paid a bribe



2 Transparency International. (n.d.) www.transparency.org/country/PH

3 Gonzales, C. (2019, October 15). *Cybercrime on the rise over the last 6 years.* Inquirer. https://newsinfo.inquirer.net/1177832/cybercrime-on-the-rise-over-the-last-6-years

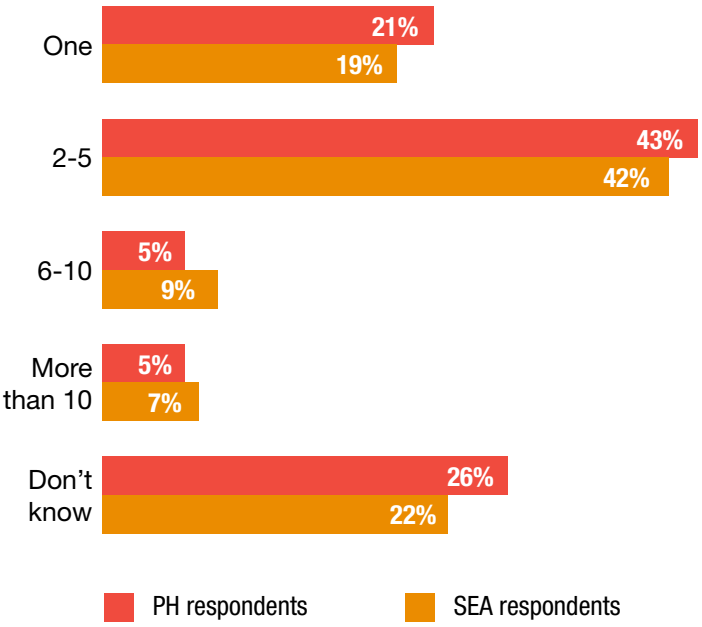
The impact and aftermath

In 2020, almost half of the respondents said that between two and five incidents occurred within the last 24 months and 26% are not aware how many incidents have happened. This may mean that not everyone in the organization is aware of how much fraud incidents are happening in their company. Quite often, once these cases come to light, management tries to keep informed employees at a minimum. There are cases too sensitive that even some top executives are kept in the dark.

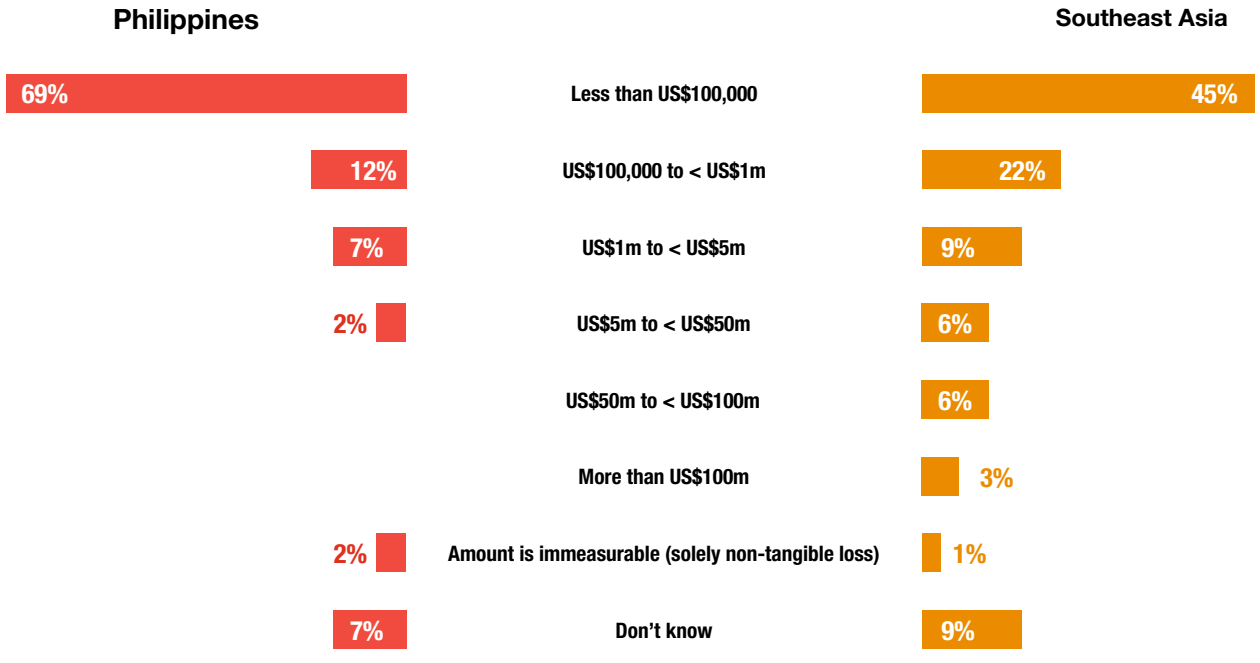
Majority of these fraud incidents amount to an average loss of up to US$100,000 per business in the past 24 months. 31% of incidents cost between US$50,000 to US$100,000. Still, there are few incidents that drain Philippines businesses of up to USD$50m. Aside from these, there are losses that may have a long-term impact and may be almost immeasurable such as loss of public trust, damage to the brand, low employee morale, and credit loss.

One out of three respondents said they were frustrated, worried and stressed out by fraud incidents in their company. No one said they were prepared.

How many incidents of fraud, corruption or other crime has your organization experienced within the last 24 months?



In financial terms, approximately, how much do you think your organization may have directly lost through all incidents of fraud, corruption or other economic crime over the last 24 months?



Who did it?

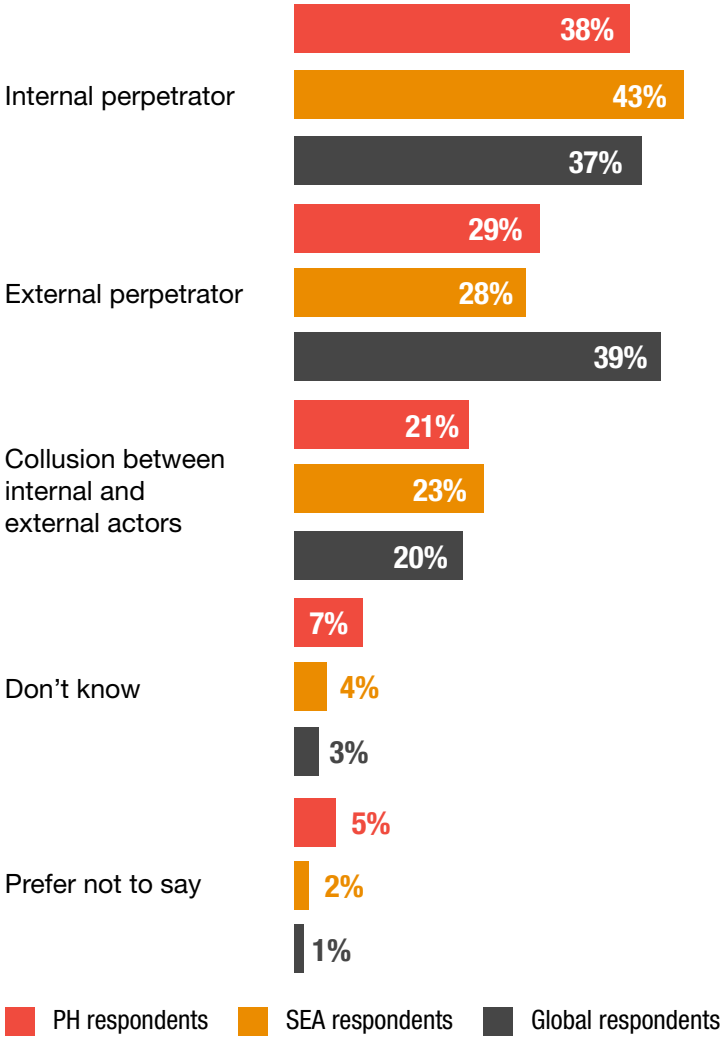
As organizations strengthen security from external forces, they should also be vigilant against spies, traitors and conspirators from within.

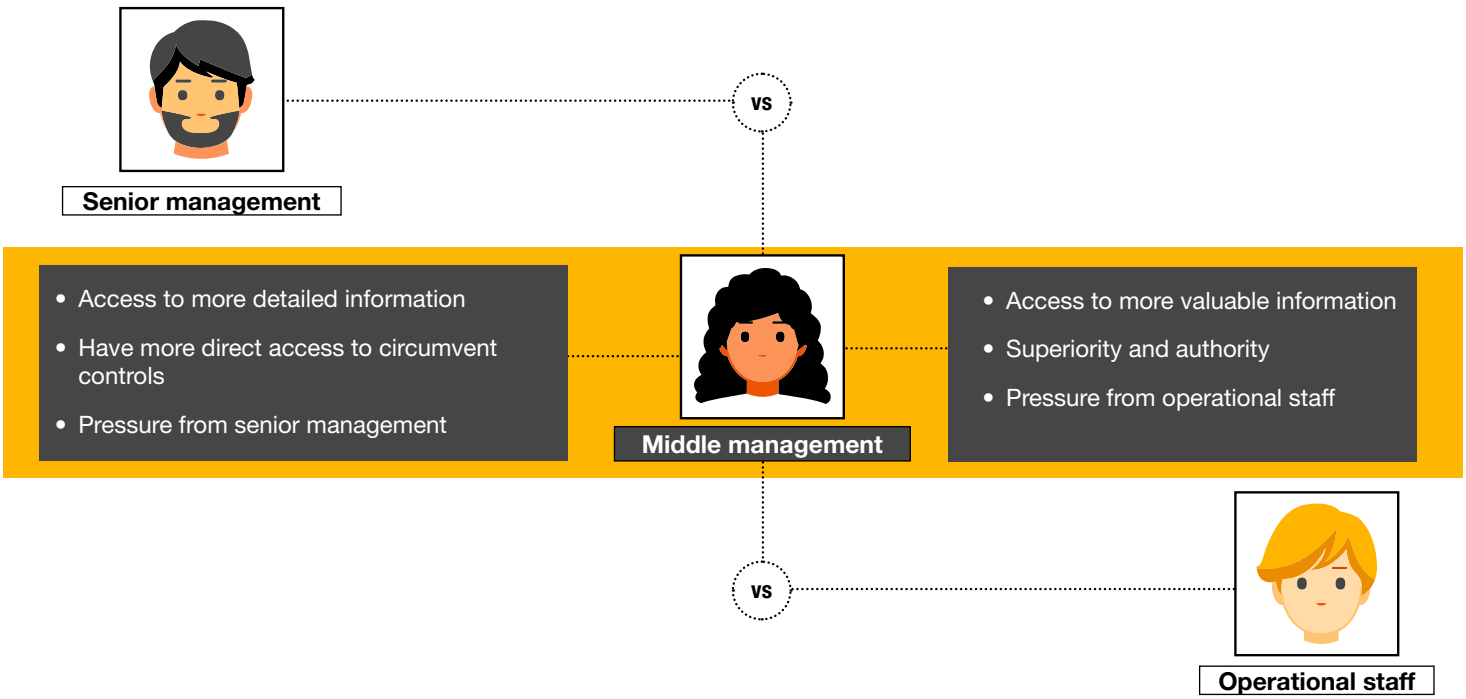
Majority of cases come from employees acting badly at night. 38% of incidents for the past 24 months are perpetrated from within the company. Shockingly, the biggest fraud incidents come from people who have been working in the company for almost half their lives but yet gave in to pressure, rationalization, and opportunity to commit fraud.

In 2016, RCBC was allegedly involved in the Bangladesh cyber heist. Investigations revealed a conspiracy that reportedly implicated one of the bank's branch managers. This ultimately resulted in the bank getting fined a record amount of PHP1bn (equivalent to about US$19.17m) in penalties, and the branch manager sentenced by the lower court with four to seven years in prison for each of the eight counts of money laundering. (The case is currently under appeal.)

Whether it was top management, operational staff or middle management – the information accessed by internal perpetrators are immense. This is why they are more successful in committing fraud than external perpetrators. As organizations strengthen security against external forces, they must also be vigilant against spies, traitors and conspirators from within.

Who was the main perpetrator of this incident?

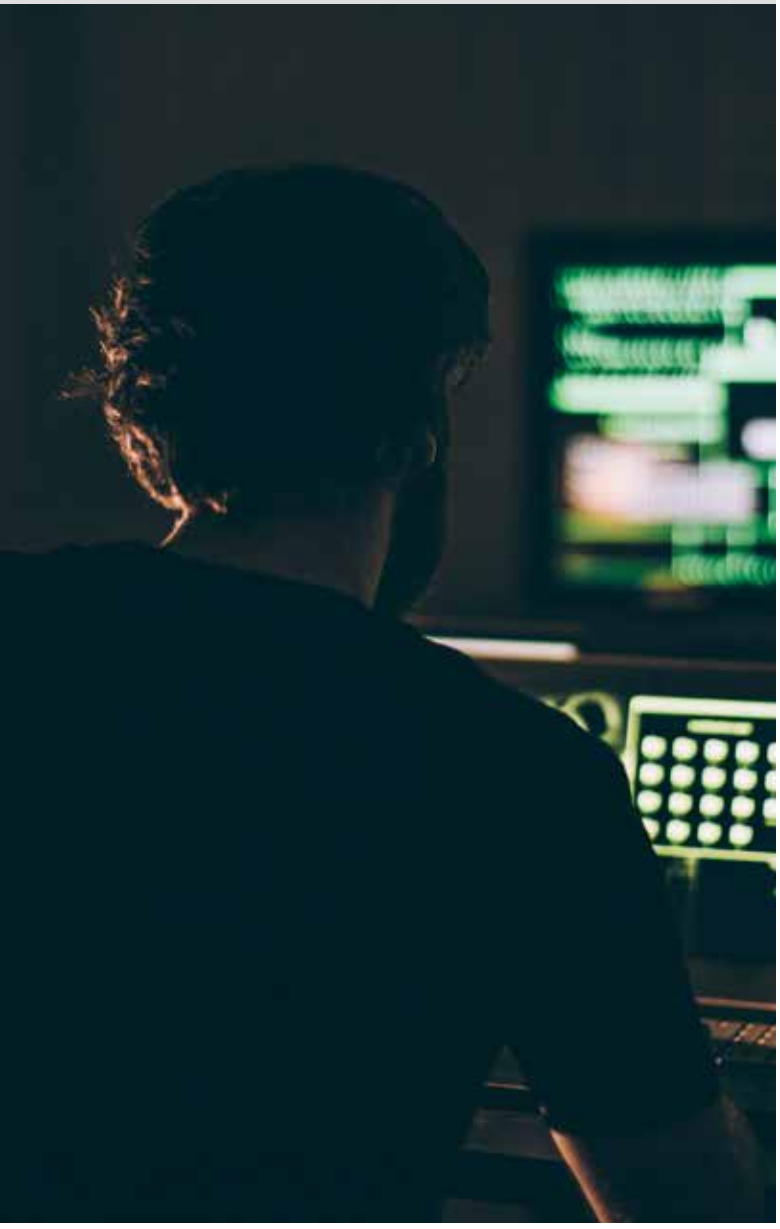




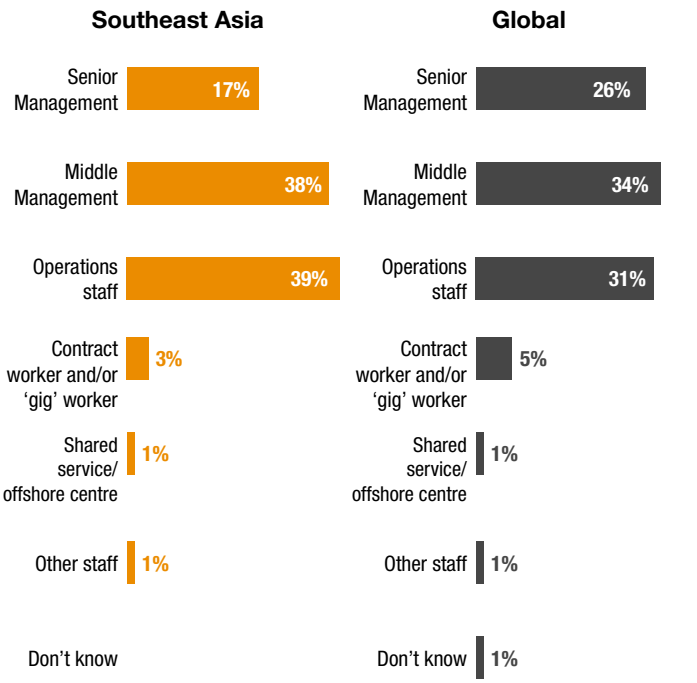
Internal perpetrators are mostly from middle management and to some extent, operations staff. Why is middle management the usual suspect? Middle management, to a certain degree, may have more fraud opportunity than both senior management and operational staff. At the same time, the pressure coming from above and below can motivate them to commit fraud.

External perpetrators usually come from vendors, customers and hackers.

Hackers – these may make up the fraudsters of the new decade, consistent with the rising case of cyber threats and crimes in the Philippines as well as across the globe. As businesses move to the digital space, so do the thieves. For hackers, data is the pot of gold. Data compromised can mean a lot of things—from requesting a fake fund transfer to infiltration of the entire system. It takes one attack to lose so much to hackers.

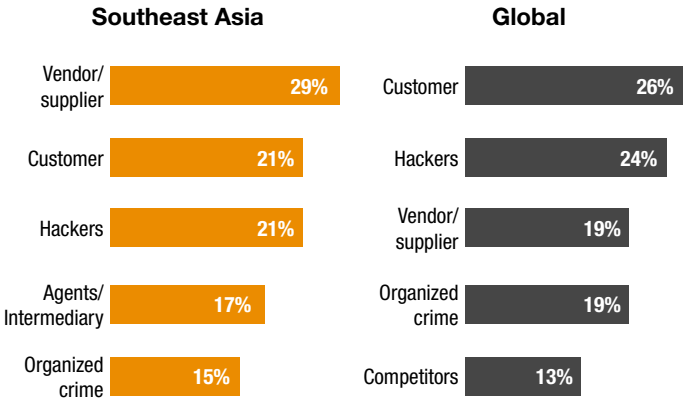


At what level, within your organization, was the internal perpetrator of this incident?



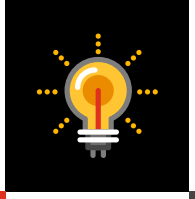
Note Philippine data is not presented due to low number of respondents. Presented instead are Southeast Asian and global results.

Who was/were the external perpetrator(s) of this incident against your organization?



Note Philippine data is not presented due to low number of respondents. Presented instead are Southeast Asian and global results.

Discovery and recovery



A few years back, the common theme of various business forums was the "future" that is 2020. Today is that year that we have been looking forward to experiencing. In our economic crime battle years ago, did we get to what we envisioned for 2020? Can we say that we are emerging stronger in fighting fraud, corruption and other economic crimes?

Same place, different times?

Over time, our study had showed us that Philippine businesses follow the same route as before on the detection, response and remediation. Illustrated below is the usual ways of detection, how to respond and the remediation program.

From this information, the Philippines appears to be moving to a better position through time in the battle of economic crime with a smarter approach in detecting and responding to incidents. However, is our pace fast enough to outsmart fraudsters? In the question *'How did your organization remediate the incident?'*, the answer *'Introduced new technologies'* fell to the bottom, with only 14% of respondents appearing to take initiatives for technology-enabled fraud fighting tools.

The Microsoft Asia Workplace 2020 (MAW2020) study shows that organizations' may not be doing enough to assist employees in coping with digital trends. Forty-seven percent (47%) reported on their organization's inadequate actions to upskill them in technology that's essential to fight economic crime.

Ways of Detection	How to Respond	Remediation
Tip-off	Conducting investigation	Enhanced controls
Suspicious activity monitoring	Disclosed to board	Enhanced policies and procedures
Account recon/Document exam	Disclosed to auditor	Disciplined/terminated employee

"Tipping-off" remains to be the main source of information in detecting irregular activities in the organization. While internal audit routine was the secondary source of leads from the previous report, this time, new ways of detecting incidents emerged as effective in discovering potential misconducts.

As a usual response, organizations are likely to jump into a fact-finding investigation to learn how the incident happened. It is also good to see that upon discovery, such incidents are being brought to the attention of relevant stakeholders who can assist in responding to the situation. The board can mobilize the organization's resources form an investigative task force. Meanwhile, the auditor can provide initial insight on its impact to the organization that will be used in making informed decisions.

The typical response: the remediating steps enhance governance and controls. Open opportunities and gaps are then being closed to avoid similar events from happening.

developed good practice

Enabling technology

Organizations incur millions of pesos in recovering from incidents to save its name and the business. Not everyone, though, is willing to spend that much money to invest in technology. Ironically, such technology can potentially save them more money and prevent further damage due to unexpected events in the future.

In the Southeast Asian region, cost is the main reason (25% of respondents) why organizations are prevented from implementing or upgrading their technology in combating fraud, corruption and other economic crimes. This may likely be the same reason why disruptive and advanced technologies are the least considered solutions by our Filipino respondents in fighting economic crimes.

The ultimate goal is to protect the welfare of the business while avoiding fraud-related costs as much as possible despite fraud risks being indelible.

Investments on fraud-fighting tools may often be perceived as a sophisticated solution. It is important to remember that every investment has returns. In the case of investing in preventive tools, its return is directly attributable to reduced fraud risk and costs when attacks strike.

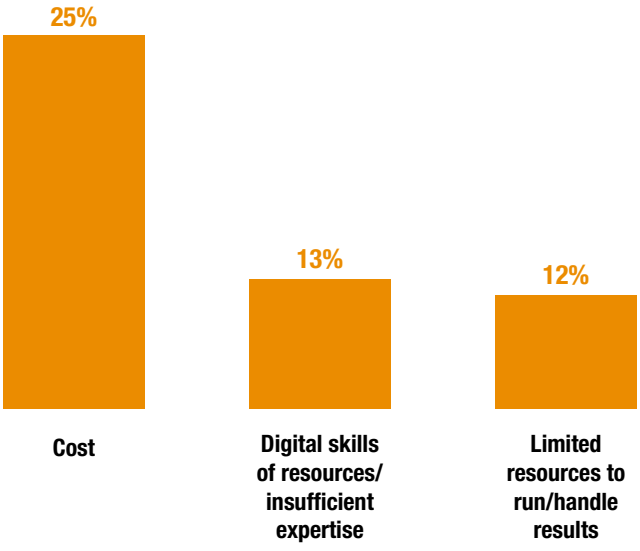
Although emerging technologies appear to be less appreciated in the Philippines, we still have to acknowledge the milestones in the aspect of digitization, including our proactive start in technological upgrades in detecting and preventing economic crimes. Across industries, especially banking, there is an increasing focus on the use, deployment and enhancement of a broad range of risk management systems, allowing proactive detection and, to a certain extent, prevention of economic crime components. Specific applications include AML systems for covered and suspicious transaction reporting and monitoring which, while in use since late 2000s, are slowly getting a capability boost through artificial intelligence, machine learning and intelligent process automation. The use of ICT for eKYC–capturing and recording customer personal data, as well as for the conduct of face-to-face contact/interview–has been enabled by BSP Circular 950. From a broader corporate landscape, companies have initiated whistleblowing platforms driven by corporate strategies, or as part of the whistleblowing framework espoused by the latest SEC Code of Corporate Governance for publicly listed companies.

Integrated Governance, Risk and Compliance (GRC) systems are likewise being deployed to capture risk assessments and incidents, facilitating detection, resolution and prevention of future occurrences.

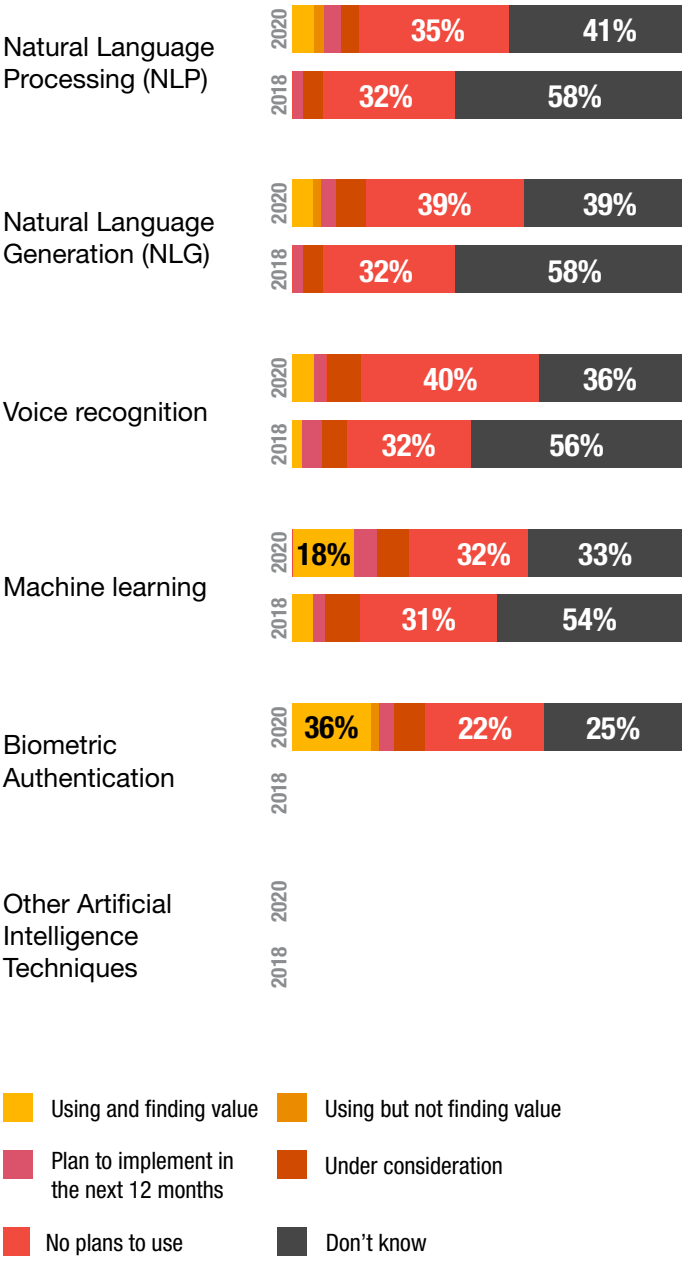
The Philippines is becoming a hub in fighting financial crime

The Philippines is slowly becoming a hub in fighting financial crime. Some large financial institutions have even offshored parts of their Know-Your-Customer/Anti-Money Laundering functions here in the Philippines.

What is preventing your organization from implementing/upgrading technology in order to combat fraud, corruption or other economic crime?



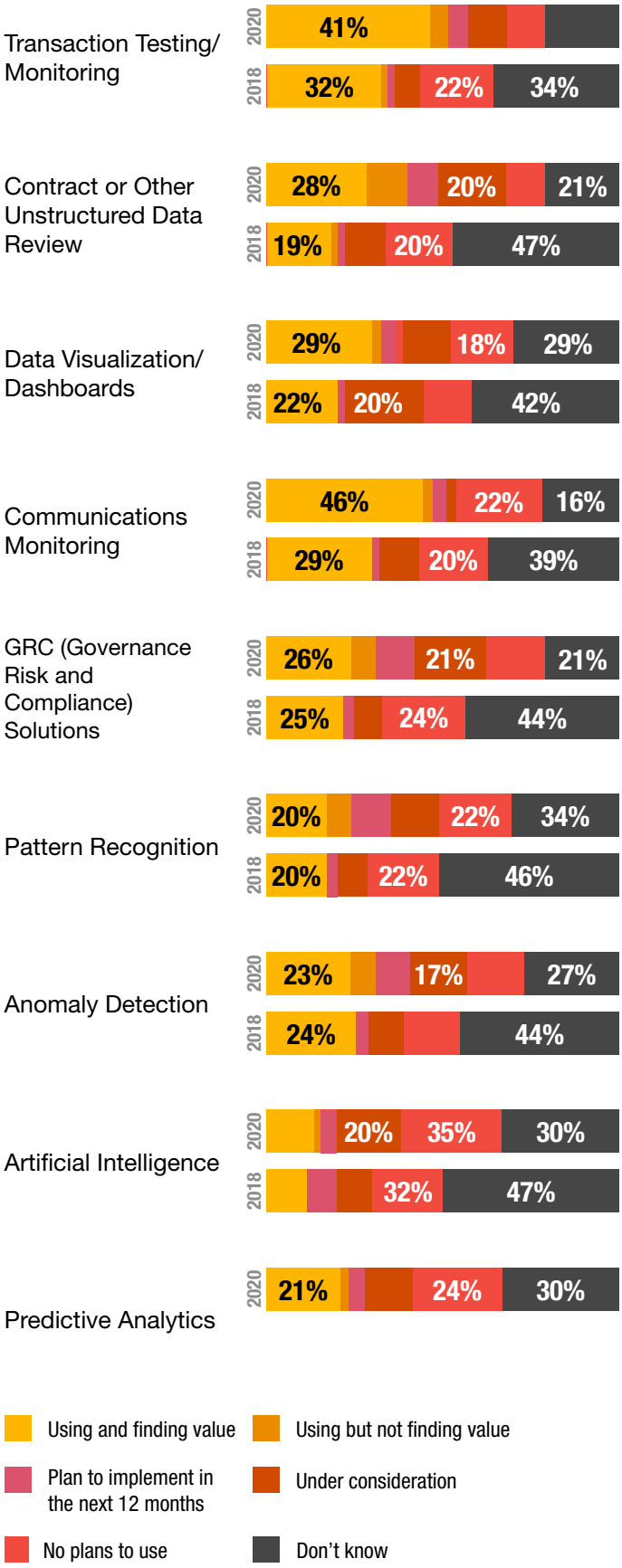
To what degree is your organization leveraging Artificial Intelligence (AI) to combat/monitor for fraud, corruption and/or other economic crimes?



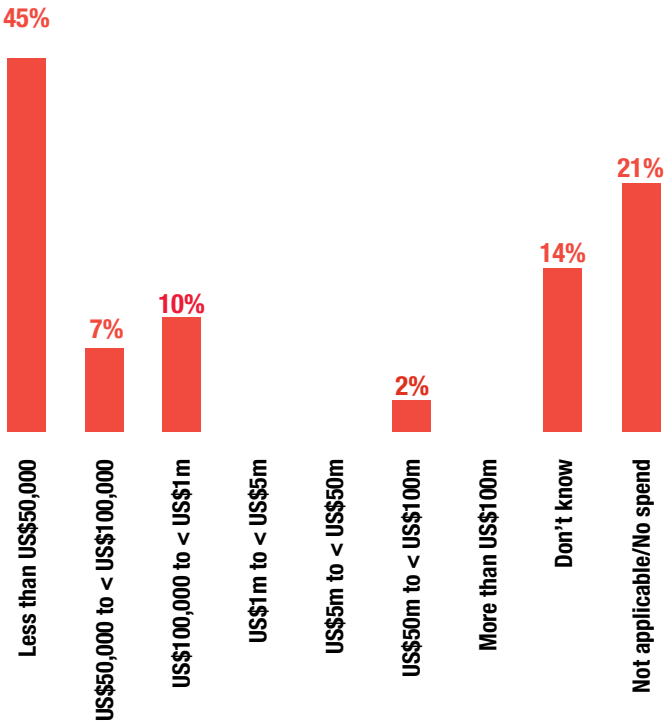
It can be observed that the majority of respondents find little value in leveraging Artificial Intelligence (AI) for fighting fraud. A large number among majority do not even intend to use AI over the next 12 months.

In contrast, a bigger proportion of respondents have found value in using alternative or disruptive technologies and techniques to further enhance how they deal with economic crime and fraud, as well as be ahead of the competition.

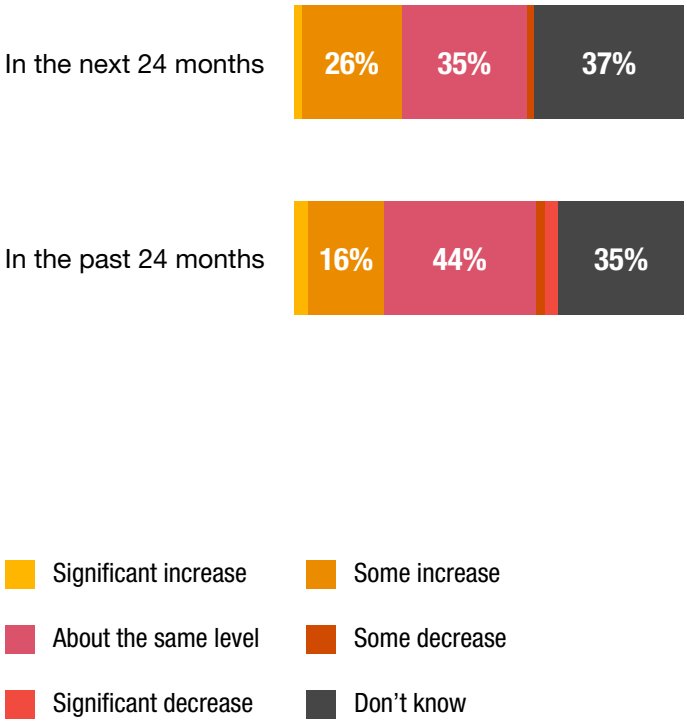
To what degree is your organization using or considering the following alternative/disruptive technologies and techniques in your control environment to help combat fraud, corruption and/or other economic crimes?



In relation to the incident experienced in the last 24 months, how much was spent by your organization on the following aspects?



How has/is your organization adjusting the amount of funds used to combat fraud, corruption and other economic crime?



With high technology, comes high responsibility – disruptive technologies for financial inclusion are open to cybersecurity threats while old-fashioned forms of fraud may be neglected when attention goes to new waves of fraud.

Despite our upgrades, we have to remember how, in the early 2000s, we looked at 2020, when everything would be possible. However, being tech-savvy does not make one invulnerable to any form of fraud, especially now where resources to commit economic crime have become accessible and affordable.

Therefore, even though 88% of Filipinos are technology-literate based on a study[4], we have to be aware that technology only enables us to be equipped but one must be unwavering in his responsibility to be vigilant at all times.

Anticipation is prevention

Technology is just one of the success factors for us to win this battle. Technology will be useless if we cannot see the bigger picture of how perpetration can happen.

In the Philippines, our overall fraud program appears to be on par with our neighbors in Southeast Asia. Fraud programs, however, will be affected by business objectives and the risks inherent to the nature of business. Therefore, for any business pursuit or route to market, the organization must anticipate the vulnerabilities that come along with its choices in order to know how to best prepare and respond accordingly. After all, it is not only a question of "if" but rather "when" organizations will experience an attack.

Since we acknowledge that fraud risks may not be 100% eliminated in every organization, the following are critical areas we must regularly look into to anticipate fraud and be ready to respond:

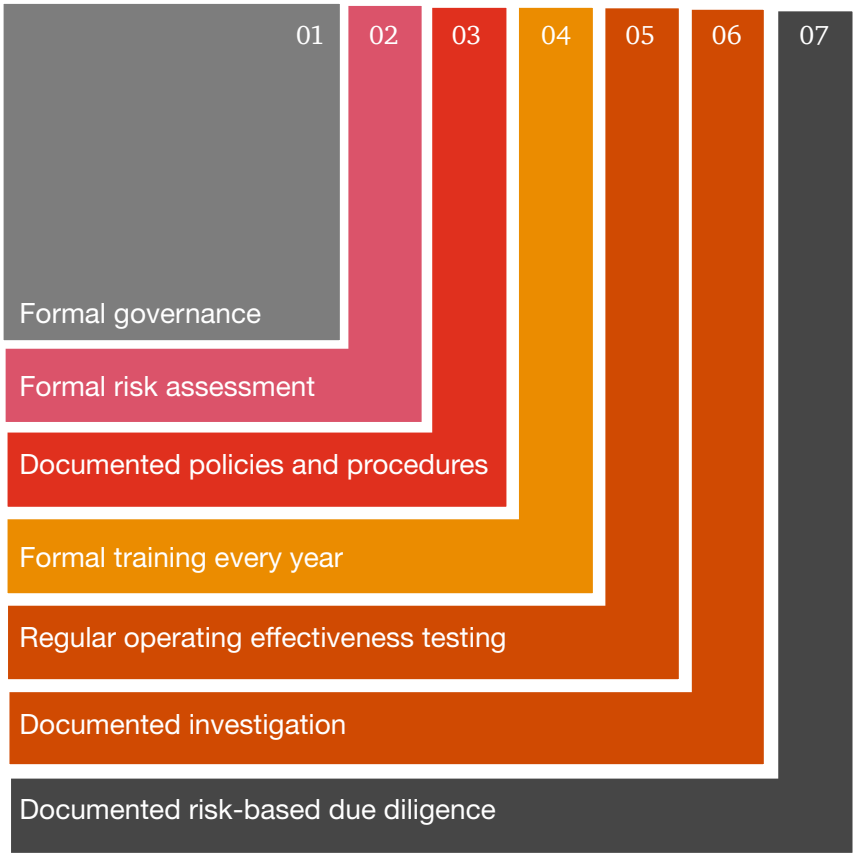
Make sense of your data. Oftentimes, organizations are unaware of the level of insight they can draw from the data available to them within their systems. By knowing how to read and draw conclusions from the data, organizations will, organizations will be able to diagnose potential fraud risks relevant to its business.

Identify opportunities to defraud. Organizations must take a proactive role in identifying fraud opportunities in order to prevent it from happening or be prepared for it when it happens.

Upskill people with technology. As important as technology is for people to be equipped with the right set of skills and knowledge. The people will man the governance structure that is the backbone of any technological initiative.

React effectively. When we anticipate, we know what to do next. We must be able to react effectively to incidents by quickly mobilizing the right resources to investigate and gather facts.

PH trend with regard to overall fraud program



4 Maghirang, T. (2019, March 24). *Get ready for tech-savvy Gen Z!.* The Manila Times. https://www.manilatimes.net/2019/03/24/business/sunday-business-i-t/get-ready-for-tech-savvy-gen-z/530014/

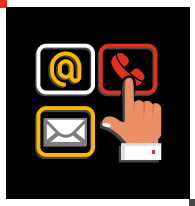
In conclusion

Philippine businesses appear to have positive outlook despite the incidents. The experience has taught us to be prepared and later on, emerge stronger. Almost 60% feel that they are now in a better position after experiencing fraud incident in their organizations.

Surely, our efforts have come a long way. It may be a slow pace but clearly, there's hope. In this report, you can find positive trends and learnings that encourage growth in our mission to fight fraud and economic crime. While the future we look forward to is now here, let us be mindful of our history so it won't repeat itself– at least, those that hurt us.

To learn more

Better understand your economic crime and fraud risks and assess your programs against your peers and our global respondents.



Alexander B. Cabrera
Chairman & Senior Partner
alex.cabrera@pwc.com
+63 (2) 8459 2002

Benjamin B. Azada
Consulting Managing Partner
benjamin.azada@pwc.com
+63 (2) 8459 3011

Roberto C. Bassig
Consulting Partner
roberto.c.bassig@pwc.com
+63 (2) 8459 3143

Veronica R. Bartolome
Consulting Partner
veronica.r.bartolome@pwc.com
+63 (2) 8459 3238

Aurelio Mari G. Gueco
Consulting Senior Manager
aurelio.mari.gueco@pwc.com
+63 (2) 8845 2728 ext. 4892

Mark Aurelius V. Bantay
Consulting Senior Manager
mark.aurelius.bantay@pwc.com
+63 (2) 8845 2728 ext. 3236

Ann Karla V. Chichioco
Consulting Manager
ann.karla.chichioco@pwc.com
+63 (2) 8845 2728 ext. 3061

© 2020 PricewaterhouseCoopers Consulting Services Philippines Co. Ltd. All rights reserved.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to a PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.