Fraud and corruption – driving away talent?

Asia-Pacific Fraud Survey 2015
In February 2015, our researchers — the global market research agency Ipsos — conducted 1,508 interviews in 14 territories in Asia-Pacific with employees working in large companies. Respondents comprised 19% senior management, 38% middle management and 43% employees.
Given the ongoing war for talent in Asia-Pacific (APAC), our APAC Fraud Survey 2015 reveals a compelling new reason for executives and boards to revisit their fraud, bribery and corruption risk mitigation strategies. To date, the incentives to get compliance right have centered on minimizing financial losses, reducing the management time required to investigate and remediate issues, and preventing the reputational damage caused by corruption.

But with a vast majority of our more than 1,500 respondents rating ethical practices as important – and nearly 80% saying they would be unwilling to work for organizations involved in bribery and corruption – there’s a new imperative to manage fraud, bribery and corruption risks effectively. Failing to do so could see promising talent avoid working for organizations and cause the best employees to jump ship, leading to higher attrition rates and expensive recruitment campaigns. In markets where it’s already difficult to recruit and retain staff, the consequences could be catastrophic.

As this survey discusses, to avoid putting their valued talent and growth strategies at risk, APAC companies will need a holistic fraud prevention and detection framework – backed by strong leadership, with up-to-date and well-enforced internal controls, policies and procedures. Organizations also need to improve the way they handle whistleblower hotline complaints, with far fewer respondents willing to use a hotline when compared to our 2013 survey.

Our 2015 survey also concludes that the answer to increasing regulatory enforcement and stretched in-house compliance teams lies in leveraging big data through forensic data analytics (FDA), as well as involving the entire C-suite in preparing for a possible cybercrime incident.

We hope the following results and analysis give executives and boards a valuable new perspective on leading practice in fraud, bribery and corruption risk management.

We also acknowledge and thank all of the respondents for their contributions.

Chris Fordham
Asia-Pacific Leader
Fraud Investigation & Dispute Services
Executive summary

Across APAC, compliance has never been more challenging – or more important – with 8 out of 10 respondents saying they would be unwilling to work for companies involved in bribery and corruption. In this environment, ensuring that companies have high ethical standards and use technology proactively to prevent and detect fraud, bribery and corruption will be key to both retain talent and make compliance programs more sustainable.

Compliance becomes increasingly complex

Respondents report business success is being challenged by increasing regulation and slower than expected economic growth. Half say stronger local anti-corruption enforcement is a major challenge. These expanding regulatory demands are requiring companies operating in APAC to look at increasing numbers of financial transactions and relationships in greater depth. And many need to do so with limited compliance resources.

This sentiment is particularly notable in Indonesia, Thailand and China, reflecting strong anti-corruption stances from the governments in these countries. Indonesia’s President Widodo ran for office on an anti-corruption platform. Thailand’s National Anti-Corruption Commission is demonstrating its teeth, indicting hundreds of former lawmakers. In China, the Government’s commitment to tackle official corruption has resulted in several dramatic prosecutions at senior levels – affecting both local Chinese companies and multinational firms.

At the same time the talent pool for qualified compliance professionals is limited. Discussions with heads of compliance in various industries indicate teams across APAC are finding it hard to recruit and retain compliance professionals.

Against this backdrop, we found:

Ethics are vital in the war for talent

Most respondents say they would be unwilling to work for companies involved in bribery and corruption. This surprisingly strong link between ethics and talent retention introduces a major new benefit to fraud, bribery and corruption risk management, especially for organizations with people at the core of their growth strategies. Running an ethical business is now central to attracting and retaining top talent.

Internal controls, policies and procedures are not always working

In response to increasing regulations and enhanced local enforcement, APAC companies have tightened up their internal controls. But anti-bribery/anti-corruption (ABAC) policies need to be more effective. Codes of conduct are not being followed and whistleblower programs are either missing or underused. Of particular concern is the finding that the percentage of respondents prepared to use their company’s whistleblower hotline has dropped dramatically since our 2013 survey.

Risk is building up all along the value chain

Many respondents do not grasp the extent of the fraud, bribery and corruption risks posed by third parties. Nor do they fully understand their responsibilities when it comes to economic and trade sanctions.

Top challenges to Asia-Pacific companies.

- Increased regulation: 59%
- Slower than expected growth: 58%
- Stronger local anti-corruption enforcement: 50%
- 2 in 3 respondents see commercial advantage in having a strong reputation for ethical behavior
Fraud and corruption — driving away talent?
Asia-Pacific Fraud Survey 2015

Companies also need to be aware of fraud, bribery and corruption risks in relation to transactions. Those involved in M&A need to make sure the right questions are asked and diligence is targeted on the right areas.

Big data and forensic data analytics
As a priority, APAC companies should start to adopt FDA to reinforce their fraud, bribery and corruption risk management framework. FDA integrates statistical analysis, anomaly detection, data visualization and text mining to identify unusual transactions. APAC organizations should leverage FDA to improve their ability to identify transactions that may indicate the presence of fraud, bribery and corruption, and make their in-house compliance resources more efficient and effective.

Whistleblower hotlines
Every company needs a whistleblower hotline as part of a broader fraud, bribery and corruption risk management framework. However, implementing a hotline is not enough. Employees must also be confident that their reports will be dealt with in a transparent and confidential manner — and that they will be protected from retaliation. This starts with senior management promoting ethical behavior by encouraging and supporting employees in filing complaints about misconduct.

Given our survey’s findings, APAC companies need to put in place:

**Strong ethical leadership**
Compliance starts at the top. Leadership must engage proactively in compliance activities, and demonstrate and communicate about ethical behavior. Executives must ensure the organization reacts quickly and effectively to any policy breaches, and support investment in compliance technology and training. At the board level, non-executive directors should set a challenging plan, ask tough questions and hold senior management accountable for the results.

**Strong, effective ethics policies and guidelines**
Simply having ABAC policies and codes of conduct is not enough — these policies must also lead to behavioral change. Turning policies into reality comes down to relevance. Employees need to understand what is required of them — and believe it is important. Starting points include translating codes of conduct into local languages and using local examples during ABAC training. Global organizations should be open to feedback from local offices on the challenges of dealing with changes to policies and procedures.

**Third-party due diligence**
Given the vast majority of reported US Foreign Corrupt Practices Act (FCPA) cases involve third-party intermediaries, APAC organizations need to improve their due diligence and monitoring of all third parties. This is required across a wide variety of relationships, from Joint Venture (JV) partners and material subcontractors to distributors and marketing agents. Companies also need to be aware of fraud, bribery and corruption risks in relation to transactions. Those involved in M&A need to make sure the right questions are asked and diligence is targeted on the right areas.

**Call to action**

Given our survey’s findings, APAC companies need to put in place:

**Strong ethical leadership**
Compliance starts at the top. Leadership must engage proactively in compliance activities, and demonstrate and communicate about ethical behavior. Executives must ensure the organization reacts quickly and effectively to any policy breaches, and support investment in compliance technology and training. At the board level, non-executive directors should set a challenging plan, ask tough questions and hold senior management accountable for the results.

**Strong, effective ethics policies and guidelines**
Simply having ABAC policies and codes of conduct is not enough — these policies must also lead to behavioral change. Turning policies into reality comes down to relevance. Employees need to understand what is required of them — and believe it is important. Starting points include translating codes of conduct into local languages and using local examples during ABAC training. Global organizations should be open to feedback from local offices on the challenges of dealing with changes to policies and procedures.

**Third-party due diligence**
Given the vast majority of reported US Foreign Corrupt Practices Act (FCPA) cases involve third-party intermediaries, APAC organizations need to improve their due diligence and monitoring of all third parties. This is required across a wide variety of relationships, from Joint Venture (JV) partners and material subcontractors to distributors and marketing agents. Companies also need to be aware of fraud, bribery and corruption risks in relation to transactions. Those involved in M&A need to make sure the right questions are asked and diligence is targeted on the right areas.

**Big data and forensic data analytics**
As a priority, APAC companies should start to adopt FDA to reinforce their fraud, bribery and corruption risk management framework. FDA integrates statistical analysis, anomaly detection, data visualization and text mining to identify unusual transactions. APAC organizations should leverage FDA to improve their ability to identify transactions that may indicate the presence of fraud, bribery and corruption, and make their in-house compliance resources more efficient and effective.

**Whistleblower hotlines**
Every company needs a whistleblower hotline as part of a broader fraud, bribery and corruption risk management framework. However, implementing a hotline is not enough. Employees must also be confident that their reports will be dealt with in a transparent and confidential manner — and that they will be protected from retaliation. This starts with senior management promoting ethical behavior by encouraging and supporting employees in filing complaints about misconduct.

---

**45%** of companies do not have a whistleblower hotline

**1 in 4** companies do not have ABAC policies

**40%** of companies do not provide ABAC policy training
Ethics — vital in the war for talent?

Respondents, especially millennials\(^1\), say they will leave or refuse to join companies involved in bribery and corruption. This adds a new dimension to compliance. Getting it wrong will put retention and recruitment of top talent and growth strategies at risk.

Workforces highly aware of bribery and corruption

Bribery and corruption remain prevalent throughout APAC, with 6 out of 10 respondents agreeing that corruption happens widely in their countries. About half attribute this to tough economic times and competition. Perceptions of corruption vary by industry, with respondents from the life sciences sector (74%) and the extractive industries (69%) most likely to agree with this statement.

Supporting these findings, two out of three respondents say their colleagues are aware of fraudulent activities within their own organizations. Of these, 39% believe their colleagues report these activities. But 27% say that, even though their colleagues are aware of fraudulent activities, they do not report them.

Not surprisingly, therefore, almost a quarter of respondents do not have confidence in their organizations’ internal procedures to detect and prevent fraud. In addition, more than a third of respondents are worried about the increasing risk of their organizations becoming a victim of fraud over the next few years. Whistleblower hotlines are consistently identified in surveys as one of the most effective sources of fraud detection and are, in our experience, an effective alert channel. In this context, the reluctance of many respondents to use whistleblower hotlines combined with an increased perceived risk of fraud, bribery and corruption is concerning.

1 in 4 respondents say their colleagues are aware of but do not report fraudulent activities.

78% of respondents and 86% of those, who are under 25, will not work for unethical companies.

Respondents unwilling to work for companies involved in bribery and corruption

However, an even bigger issue for employers is that respondents say they do not want to work for organizations involved in bribery and corruption. When asked of their perceptions of an organization that has been involved in a major bribery or corruption case, 78% of our respondents said they would be unwilling to work for such an organization or would consider other employment opportunities. A further 16% would be willing to work for such employers, but would need reassurance about the organization’s actions to address the problem. Only 5% of respondents say it would “make no difference to their willingness to work for them.”

60% of respondents believe bribery/corrupt practices happen widely in their country.

---

\(^1\) Also known as the Millennial Generation or Generation Y, being those with birth years ranging from the early 1980s to the early 2000s.
Interestingly, the millennials – whose influx into the APAC workforce is already testing traditional HR strategies – feel most strongly about this issue. An overwhelming 86% of those respondents aged under 25 say they are unwilling to work for, or would leave, an organization involved in bribery or corruption. In contrast, around one in five respondents aged over 55 are willing to work for such a company.

78% of respondents say if an organization was involved in bribery and corruption, it would affect their willingness to work for that company.

Ethical business key to talent retention

Two-thirds of respondents think that having a good reputation for ethical behavior is a commercial advantage. Our findings demonstrate that this advantage now includes talent retention, providing a new and powerful imperative for more robust compliance.

Compliance has always been about protecting value – avoiding financial loss and reputational risk. But now it also encompasses talent: the very core of an organization, essential for its survival. Retaining talent is about more than just competitive salaries and working conditions. Employees must also have confidence that their organization will act ethically.

This means not just having compliance programs in place, but management demonstrating decisive action. For example, having a whistleblower hotline is one component. But executives also need to be seen to react quickly to whistleblower reports and to conduct fair and objective investigations. Companies must also be seen to be more proactive in identifying corrupt conduct. This includes harnessing technological advances to better leverage corporate big data and the insights it can provide into unethical behavior.

“Ethics are already high on the governance agenda, but the on-the-ground-execution of that top-down compliance message needs work, especially in local markets where regulation and enforcement trends are rapidly evolving.”

Emmanuel Vignal
Greater China Leader,
Fraud Investigation & Dispute Services

Figure 1.
Those unwilling to work for or who would definitely leave for an equal opportunity at another organization if their organization was involved in bribery and corruption

<table>
<thead>
<tr>
<th>Feeling</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>I would be unwilling to work for them</td>
<td>29%</td>
</tr>
<tr>
<td>I would definitely leave for an equal opportunity at another organization</td>
<td>18%</td>
</tr>
<tr>
<td>I would reconsider working for them and would look elsewhere for other opportunities</td>
<td>31%</td>
</tr>
<tr>
<td>I would be willing to work for them but would need reassurance about their actions to address the problem</td>
<td>16%</td>
</tr>
</tbody>
</table>

Q: Thinking about your perceptions of an organization that has been involved in a major bribery or corruption case, which, if any, of the following applies to you?

Base: All respondents (1,508)
In response to increasing regulation and enhanced local enforcement, APAC companies have strengthened their internal controls. But some policies and systems are not working as well as they should — and many companies are struggling to make compliance sustainable.

Since the last APAC Fraud Survey conducted in 2013, many more APAC organizations have established codes of conduct, ABAC policies, training, and whistleblower hotlines. Yet not all of these initiatives are achieving their objectives.

Work needed to make ABAC policies relevant and effective

The majority of APAC companies are putting elements of compliance in place. For example, more than three quarters (76%) of respondents say their company has introduced an anti-bribery policy. The question is: are these elements working?

According to respondents, the answer is: still not well enough. Encouragingly, 60% of respondents have seen their organizations take action against those who breach ABAC policies. More than half (55%) report regulators taking action against employees in their organizations for breaching ABAC regulations.

In addition, more respondents in our survey in 2015 than in 2013 believe their ABAC policies are working. Two years ago, 59% of our APAC Fraud Survey 2013 respondents said their ABAC policies were neither relevant nor effective. In our APAC Fraud Survey 2015, this figure is now down to 52%. Similarly, 48% of the respondents in our APAC Fraud Survey 2013 said the policy was, “…good in principle but does not work well in practice.” In our 2015 survey, this figure is now 30%, suggesting that progress is being made.

However, some respondents have doubts about their ABAC policies with 27% agreeing with the statement, “If we followed our ABAC policy very closely, it would harm our competitiveness in our local market.” Also, despite 70% of our respondents saying that senior management has “strongly communicated its commitment to our anti-bribery policies,” the evidence suggests that not everyone is “walking the talk.”

The 2014 EY Global Fraud Survey of more than 2,700 executives found 42% thought that at least one of a questionable list of actions (including giving cash payments to win business and misstating financial performance) is justified. Our APAC Fraud survey 2015 backs up this finding. Almost half (48%) of respondents think their local management is likely to act unethically during difficult times. Four out of ten respondents have also seen people with questionable ethical standards being promoted.
Codes of conduct in place but not always followed

More than 80% of respondents say their organization has a code of conduct. But 41% believe it has little impact on how people actually behave. A quarter of all respondents report that their colleagues do not comply with their organization’s code of conduct. More than half (57%) of respondents think their code of conduct should be more flexible to accommodate local needs.

These findings reinforce the importance of translating codes of conduct into the local language and localizing the training to ensure employees understand their relevance.

Figure 3. Opinions of ABAC policies

<table>
<thead>
<tr>
<th></th>
<th>52%</th>
<th>30%</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is neither relevant nor effective</td>
<td></td>
<td></td>
</tr>
<tr>
<td>It is good in principle but does not work well in practice</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q: Which, if any, of the following applies to your organization’s ABAC policy?
Base: Respondents whose companies have ABAC policies (1,142)

Global organizations should be open to feedback from local offices on the challenges of dealing with changes to policies and procedures. Companies should be wary of policy documents that are exceedingly long. Wording should be in plain language — where possible avoiding legal terminology, which will be unfamiliar to many local employees. Localized training should be set in the context of current issues. It must be highly specific on how enforcement and compliance affects the participants’ company and the responsibilities of their individual roles.

1 in 4 respondents say that their colleagues do not comply with their organization’s code of conduct.

2 in 5 respondents say their code of conduct has little impact on how people actually behave.

Figure 4. Employees complying with codes of conduct

<table>
<thead>
<tr>
<th></th>
<th>3%</th>
<th>5%</th>
<th>17%</th>
<th>45%</th>
<th>30%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tend to disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Neither agree nor disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tend to agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strongly agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q: Please indicate how much you agree with the statement: “Employees in my organization comply with the code of conduct”
Base: Includes respondents whose companies have a code of conduct (1,245)
Whistleblower hotlines underused

Establishing a whistleblower hotline with proper protection of the whistleblowers will result in more people “doing the right thing”; yet our APAC Fraud Survey 2015 still finds that 45% of companies in APAC have yet to implement a hotline.

In our experience, a company’s whistleblower hotline is often seen by the employees as management’s visible commitment to ethical behavior. Having a whistleblower hotline that employees trust and are prepared to use without fear of retaliation sends a clear message that the company will not tolerate unethical behavior.

Only around half of the respondents said that they would be prepared to use their company’s whistleblower hotline, and this compared with more than 80% of respondents in our APAC Fraud Survey 2013. This drop appears to be due to respondents being increasingly concerned about the insufficient legal protection and/or the lack of confidentiality for whistleblowers. Whether there are protections in law or not, the whistleblower policies need to reassure employees that they will get the protection and confidentiality they need.

Figure 5.
Decrease in the number of respondents prepared to use a whistleblower hotline

<table>
<thead>
<tr>
<th>Year</th>
<th>Percentage Prepared to Use Whistleblower Hotline</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>81%</td>
</tr>
<tr>
<td>2015</td>
<td>53%</td>
</tr>
</tbody>
</table>

Q: Which, if any of the following would characterize your willingness to use a whistleblower hotline: “I would be prepared to use it”

2013 Base: Respondents whose companies have a whistleblower hotline (245)
2015 Base: Respondents whose companies have a whistleblower hotline (828)

“Whistleblowers often have documents to back up their claims, but they rarely share this information in their early reports. Frequently, the whole story does not come out until investigators have had several discussions and have earned the trust of the person who has come forward.”

Diana Shin
Partner, Fraud Investigation & Dispute Services, China

Making your whistleblower program work

Companies should introduce whistleblower hotlines as a key element in a broader fraud, bribery and corruption prevention and detection framework. However, implementing a hotline is not enough. Organizations must also take the following steps to make sure employees have confidence to use the hotline:

- **Set the tone at the top** – promote ethical behavior by encouraging and supporting employees in filing complaints about misconduct.
- **Preserve confidentiality** – as permitted by applicable laws and professional standards.
- **Protect whistleblowers** – the whistleblower policy should actively protect users from retaliation, regardless of the existence of any local laws that also protect them.
- **Have a whistleblower report response plan** – the whistleblower policy also needs to demonstrate that reports will be handled objectively and with proper oversight.
- **React quickly** – contact the whistleblower immediately; establish a direct line of (preferably) face-to-face communication with someone the whistleblower trusts.
- **Consider using an independent third party** – to contact the whistleblower; more than 60% of respondents said they would be more comfortable communicating with someone from outside the company.
- **Set the right example** – if allegations are substantiated, take appropriate disciplinary action and communicate the results across the organization as appropriate.
- **Establish oversight by independent non-executive directors (INEDs)** – who should have access to appropriate resources to fulfill their responsibilities, including the ability to engage with outside counsel, forensic accountants or other professional advisors.
- **Give whistleblowers access to the Compliance Officer** – who in turn should have direct access to the INEDs.
Fraud and corruption — driving away talent?
Asia-Pacific Fraud Survey 2015

Risk-based approach to bribery and corruption using Forensic Data Analytics (FDA)

ABAC policies, codes of conduct and whistleblower hotlines are just the starting point for building an ethical business. All of these tools need to exist within a holistic fraud management framework, driven by strong leadership, and connected and backed by technology.

As a priority, APAC companies should start to adopt forensic data analytics (FDA) to reinforce their fraud, bribery and corruption risk management framework. FDA uses financial accounting data and unstructured data such as emails to quickly target high risk areas for internal audit and compliance testing. FDA enhances both the risk assessment and monitoring processes to help identify potentially unethical activity and suspicious transactions. Fundamentally, an unbiased filter can be applied to large volumes of data that would otherwise have required lengthy and costly manual review and human interpretation.

More efficient and cost effective sampling and auditing

FDA is designed to highlight suspicious or potentially improper activity before on-site visits. Armed with insights mined from corporate big data, time in the field is better targeted and spent on sampling and auditing the identified high risk areas.

With greater demand for internal audit and compliance testing, and with limited supply of skilled resources, internal audit and compliance functions are under significant pressure. FDA will help to make compliance programs more efficient and cost effective.

“Forensically analyzing and applying visualization to hundreds of millions of company transactions in order to quickly spot patterns and outliers of potential fraud can save millions of dollars in losses, as well as protecting reputations.”

Jack Jia
Partner, Fraud Investigation & Dispute Services, Hong Kong

FDA Case Study

EY helped a global pharmaceutical company use advanced FDA tools to monitor and detect potential fraud in nearly 30 countries on 6 continents involving hundreds of employees.

The project involved:
- Strengthening on-going fraud monitoring program by integrating multiple data sources (unstructured and structured)
- Collecting data from more than 300 custodians
- Loading 2,000 gigabytes of data onto a review platform
- Culling down more than 25 million documents to 1.3 million documents, which were then reviewed.
- Examining more than 2 billion financial transactions across general ledger, accounts payable, and travel and entertainment
- Handling 20 different systems of accounting for more than 30 separate business units
- Customizing EY’s proprietary fraud library to meet the client’s compliance program needs

The client is now much more effective and efficient in identifying potentially improper payments and high-risk vendors and employees across its worldwide operations.

Example of an analytic dashboard

Life Sciences Integrated Compliance Analytics Dashboard
Accounts Payable: Travel and Entertainment

[Image of analytic dashboard with Travel Locations and Summary by Employee (Sized by Amount)]
Many respondents do not grasp the extent of the fraud, bribery and corruption risks related to third parties. Nor do most respondents understand their responsibilities when it comes to economic and trade sanctions.

More due diligence required to manage third-party risks

More than half of the respondents think third parties are a risk to their business in relation to ABAC compliance. Such third parties include JV partners, distributors, agents and vendors. However, the majority believe their companies are capable of handling this risk, with nearly three-quarters (72%) being confident that their organization is effectively managing the fraud, bribery and corruption risks associated with these third parties.

However, we believe such confidence may be misplaced. The FCPA enforcement actions brought by the US Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) demonstrate that third parties, including agents, consultants, and distributors, are commonly used to conceal the payment of bribes to foreign officials in international business transactions. It is possible that respondents are overestimating their organization's ability to manage third-party risks. It is recommended that guidance such as ‘A Resource Guide to the FCPA U.S. Foreign Corrupt Practices Act’ prepared by the U.S. DOJ and the Enforcement Division of the U.S. SEC should be part of the foundation of any policy and procedure formulation or design of educational content.

This overconfidence is especially likely if organizations do not fully understand the extent of subcontracting arrangements being entered into, either by their own third-party providers or by a JV partner. In these circumstances, third-party fraud, bribery and corruption risks are heightened considerably.

Joint venture partners

Respondents are most concerned about the bribery and corruption risks associated with JVs. When one considers the potential reputation damage and economic losses associated with an FCPA breach by a JV partner, this concern is well founded.

For example, if an obscure JV partner of a well-known brand is caught bribing a foreign official, this could result in negative media coverage that is more likely to associate the offence with the brand to create a more sensational story. The media coverage of the procurement fraud case at the contract manufacturer of a multinational technology company in 2013 highlighted this risk.

Anti-corruption due diligence

Companies need to be aware of fraud, bribery and corruption risks in relation to transactions. Yet according to the 2014 EY Global Fraud Survey, 40% of companies never conduct forensic or anti-corruption due diligence as part of their M&A process. This issue was in the spotlight again in November 2014, when the DOJ issued an FCPA Opinion Procedure Release for acquiring companies. The DOJ release re-emphasized the importance of conducting FCPA pre-acquisition due diligence and to implement appropriate post-acquisition integration steps in response to risks identified. The DOJ encourages acquiring companies to:

- Conduct thorough risk-based FCPA/ABAC due diligence
- Implement the acquiring company’s code of conduct and ABAC policies as quickly as practicable
- Conduct FCPA/ABAC and other relevant training for the acquired entity’s directors and employees, as well as third-party agents and partners
- Conduct an FCPA-specific review of the acquired entity operations as quickly as practicable
- Disclose to the DOJ any corrupt payments discovered during the above procedures

In our experience, significant bribery and corruption risks can fall through the cracks if the right questions are not considered or diligence is not targeted on the right areas. Wherever possible, these questions should be asked at the pre-acquisition stage and appropriate background checks of management and third parties can be conducted. We recognize that in many situations, full access to company records is not provided during due diligence. We highly recommend that companies expand their ABAC diligence as the deal progresses. Often, additional access is gained between signing and closing. Focused interviews, transaction testing and analysis are ideally accomplished pre-closing. However, at a minimum, a detailed plan should be developed pre-close to assist in identifying potential risks post-close. But, if they are not, a limited window (of 180 days according to the DOJ’s 2008 Halliburton FCPA opinion release) exists to do so post-acquisition – as long as the acquirer has taken reasonably prudent steps pre-closing.

---

Given the legal and reputational exposure it creates, entering into a JV or business relationship requires as much due diligence as an acquisition, if not more, since companies will have limited operational control and oversight over the third party and its activities. To defend themselves against third-party transgressions, APAC companies need to be able to implement robust due diligence procedures and incorporate third-party/subcontractor disclosure requirements into any contractual arrangement with a commercial partner. APAC companies must demonstrate that reasonable efforts were made to assess partners, not just to ensure they have ABAC policies, but to understand the impact of updates, to know which changes to prioritize and to ensure they are applied correctly.

**Local vendors and suppliers**

Over half (56%) of respondents are aware of the risks to their business in relation to fraud, bribery and corruption from vendors and suppliers. Part of the issue in managing these risks is the sheer volume of information sources now available for vetting the risk profiles of third parties and their executives. This can be a challenge for stretched in-house compliance or legal teams who sometimes struggle to manage initial and ongoing supplier due diligence.

Third-party relationships need to be continually monitored and assessed. This may include updating existing due diligence procedures, providing regular training, conducting compliance health checks and risk assessments and exercising audit rights.

**Meeting the challenge of integrity diligence**

Integrity diligence involves, among other things, understanding the qualifications and associations of a third party, including its business reputation and any relationships with government officials. This can involve searching more than 200 open source databases, as well as economic and trade sanctions lists, litigation lists, adverse media reports and a third party’s connections to state-owned enterprises and politically exposed persons.

To do so efficiently and effectively, the degree of scrutiny should be risk-based, conducting additional research if red flags surface. It must also comply with local laws concerning data privacy and collection.

For example, EY Integrity Diligence offers a tiered approach to background diligence, compliant with the laws in each jurisdiction.

<table>
<thead>
<tr>
<th>Research</th>
<th>Quick scan</th>
<th>Level I</th>
<th>Level II</th>
<th>Level III</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online watchlist Adverse media check</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Detailed online company and executive background research, performed at the global and local levels</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Localized public records archive search, such as local court filings</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Field research, such as site visits and interviews</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

EY also uses a web-based technology platform, EY_ID, to help manage the diligence process. This interactive decision management tool stores information related to the entire third-party onboarding process in a single searchable database. Third-party questionnaires, risk ratings, background diligence results, compliance certifications and contracts, as well as the necessary internal approvals, become easily accessible in this interactive platform.
Economic sanctions poorly understood

Multinational companies need to be aware of economic and trade sanctions legislation and how to comply with it. At its core, sanctions compliance involves screening financial transactions and business dealings against constantly evolving sanctions lists of companies and individuals. Keeping sanctions lists accurate and up-to-date can be challenging and expensive. The complex nature of this information can make it difficult to understand the impact of list updates, to know which changes to prioritize and to ensure they are applied correctly.

The consequences of being found guilty of breaching economic and trade sanctions are serious. A number of financial institutions have been subject to fines and settlements with regulators for such breaches that total in the billions of US dollars.

Yet around 40% of respondents say they do not understand the importance and impact of sanctions or the consequences of dealing with parties on the sanctions lists. One-third of respondents do not appear to consider the risks of doing business with parties that may have relationships in countries on the sanctions lists.

Understanding of this issue varies by industry, with some sectors demonstrating higher levels of awareness than others. Not surprisingly, after financial institutions were subject to record fines for sanctions violations in 2014, respondents in financial services showed the highest understanding of the importance of sanctions. Interestingly, those respondents from extractive industries had a similar level of awareness, however, it is concerning that a third of the respondents in these sectors still report that they have a limited understanding of sanctions violations.

APAC companies need to make sure their employees understand the extent to which they may be inadvertently caught out by sanctions obligations. Also, to avoid breaching sanctions legislations, companies need to use technology, including FDA, to screen transactions as they occur. According to the US Department of Treasury’s Office of Foreign Asset Control, one offender’s procedures introduced to improve compliance has included scanning payments for sanctions violations in real time.

“The prevalence of FCPA matters involving third parties, means that organizations must understand their end-to-end value chains. That 72% of survey respondents are confident that their organizations are effectively managing the fraud, bribery and corruption risks associated with third parties tends to suggest that these risks are not fully understood or there is a misplaced belief in the effectiveness of their organization’s control framework.”

Rob Locke
Oceania Leader,
Fraud Investigation & Dispute Services

40% don’t understand the importance and impact of economic and trade sanctions

1 in 3 respondents would not consider the risks of doing business with parties that may be on sanctions lists.
The potential impact of cybercrime requires that cybersecurity be viewed as a business risk, rather than merely an IT issue. Fundamentally, because a cyber attack may affect business operations, financial statements and legal exposure, its reputation is on the line. While many businesses have increased their focus on cybersecurity, their efforts have been primarily on protecting their information by preventing breaches. Unfortunately, the current threat environment is such that it is only a matter of time before all businesses will suffer a major cyber breach.

In order to adequately address these likely large and complex breaches, it is necessary for companies to develop a strong, centralized response framework as part of the enterprise risk management strategy. A centralized, enterprise-wide cyber breach response program (CBR) is the focal point that brings together the wide variety of stakeholders that must collaborate to resolve a breach. The CBR program needs to be run by a team that is equipped with in-depth legal, compliance and technology experience, and would therefore be prepared to manage the day-to-day operational and tactical response.

In our survey, respondents with real-life experience battling cyber threats appear, however, to be less confident about their company’s preparedness. For example, less than half of our respondents in Hong Kong (41%), South Korea (43%) and Japan (48%) agree that their companies are fully prepared. Organizations need an enterprise-wide cyber breach response plan, with roles and responsibilities for key leaders defined in advance.

The potential impact from a cybercrime incident requires the participation of the entire C-suite. In particular, the General Counsel is playing an increasingly central role, as he or she will have responsibility for communicating with regulators, law enforcement, and any other government agencies – in addition to coordinating with human resources and public relations depending on the type and scope of impact. Finally, the General Counsel must also work with external counsel on any associated litigation matters, which may bring additional eDiscovery challenges.
More connectivity, more vulnerability

With organizations increasingly relying on internet-enabled platforms, cybercrime is growing ever more damaging to companies and their brands. The rising interconnectivity of people, devices and organizations – for example, via Bring Your Own Device programs, social media and cloud technology – opens up new vulnerabilities that are being exploited by hackers and cyber criminals, who are increasingly organized, sophisticated and well-funded.

We have reached a point where it is no longer possible to prevent all breaches. Even companies with strong cybersecurity policies, processes and technologies may not be well-positioned to handle emerging threats. Every organization needs not only strong defenses and detection capabilities, but the plans and processes to quickly to respond and recover from any cybercrime breach.

It is not enough to just know there are threats. The board and executive team, as well as IT, need to understand the nature of those threats and how and where these might manifest themselves, and assess any likely impacts. Incorporating external cyber threat intelligence feeds, as well as establishing an internal capability to generate cyber threat intelligence, can help answer these questions.

Out of 15 sectors surveyed, top 5 that are most concerned about cyberattacks

Out of 14 job functions surveyed, top 5 that are most concerned about cyberattacks

Cyberattack – a case study

When the FBI alerted a global manufacturing company that it had been the target of a cyber attack, EY led a multi-disciplinary investigative team that confirmed the breach and developed a response plan.

The project involved:

• Coordinating client executives from the General Counsel's Office, Security, Governance, Operations, Public Relations, and third-party vendors
• Liasoning with law enforcement agencies
• Developing and implementing specific protocols for evidence collection, preservation, analysis and reporting
• Identifying entry points, vulnerabilities attackers exploited and functionality of malicious code
• Determining immediate controls remediation needs

EY determined that the client had been a victim of an advanced persistent threat intruder. The organization now has protocols and controls in place to detect and counteract future cyberattacks of this magnitude.
Fraud and corruption — driving away talent?

Asia-Pacific Fraud Survey 2015

“IT's no longer enough to build a fence around your own organization. Cybersecurity should extend to your entire ecosystem, including clients, suppliers/vendors, business partners and alumni.”

Warren Dunn
Partner, Fraud Investigation & Dispute Services, Australia

Time to review cybersecurity against emerging threats

1. Conduct a cyber threat assessment to identify gaps and remediation measures
2. Get board level support for security transformation
3. Review and update security policies, procedures and supporting standards
4. Establish a Security Operations Center with monitoring and incident response procedures
5. Design and implement cyber breach response program
6. Test the cyber breach response program and related business continuity plans

Figure 6.
Unprepared for cyberattacks

1 in 5 disagree that their organization is fully prepared to protect itself against cyberattacks.

Q: Please indicate to what extent you agree with the following statement: “I think my organization is fully prepared to protect itself against cyberattacks”
Base: All respondents (1,508)
Conclusion

APAC is suffering a critical shortage of experienced compliance professionals as demand is outstripping supply. As a result, turnover among compliance professionals appears to be at an all time high, putting pressure on existing initiatives and making it challenging for companies to respond effectively to increasing regulatory enforcement.

Against this challenging backdrop, the prevention and detection of unethical practices have a new imperative: talent retention. This is no longer just about compliance. Organizations involved in fraud, bribery and corruption scandals may lose their top talent. The potential toll on productivity and growth strategies could be highly damaging.

As a priority, organizations should review their current fraud, bribery and corruption prevention and detection approaches through this new lens – paying particular attention to ethics in the work environment and instituting a robust fraud, bribery and corruption risk management framework, aided by forensic data analytics, to make compliance more efficient, effective and sustainable.

Call to action

1. **Strong ethical leadership**
   Leadership is vital to embedding a high level of compliance activity across an organization. It is not enough to launch a program and just show support at the start. Executives and senior managers must continuously set the example of ethical behavior and communicate proactively about it. At the board level, non-executive directors should set a challenging plan, ask tough questions and hold senior management accountable for the results.

2. **Strong, effective ethics policies and guidelines**
   Many companies now have ABAC policies and codes of conduct, but now they need to embed ethical behavior into ‘business as usual’. This will require strong leadership and proactive communication, such as including a “compliance moment” in every meeting as well as ongoing training. Employees must have greater awareness of cyber threats such as spear-phishing, which seeks either to steal specific commercial data or to wipe data completely, crippling an organization. They also need to understand their responsibilities when it comes to third-party risks and economic and trade sanctions.
Third-party due diligence
To avoid being associated with fraud, bribery and corruption, APAC organizations need to improve their integrity diligence and monitoring of all third parties. They need a consistent, practical diligence process. This should be tiered to ensure that scrutiny increases as higher risks are detected, and to include regular compliance health checks and fraud risk assessments. Companies that lack the necessary scale to resource this process should consider leveraging decision management tools. For companies involved in M&A, risk-based ABAC due diligence is also essential pre- and post-acquisition.

Big data and forensic data analytics
Large companies create millions of transactions. APAC organizations should leverage FDA, which integrates statistical analysis, anomaly detection, data visualization and text mining to analyze large numbers of transactions. Deployed over large datasets from multiple sources, FDA can help to identify unusual transactions or anomalies, learning from each finding to identify potential unethical behavior or suspicious transactions. By focusing in-house resources on high risk areas, FDA can help APAC companies increase the overall efficiency and sustainability of compliance initiatives, while improving the effectiveness of internal investigations.

Whistleblower hotlines
Whistleblower hotlines are an essential part of a broader fraud, bribery and corruption risk management framework. They are often the first channel of complaint for employees and other stakeholders. But they will only be used if employees are confident that their reports will be dealt with in a transparent and confidential manner and that they will be protected from retaliation. Given most employees would prefer to deal with someone from outside the company, APAC organizations should consider using an independent third party to receive and investigate whistleblower complaints.
Survey methodology

Between 5 and 23 February 2015, our researchers – the global market research agency Ipsos – conducted 1,508 interviews with employees of large companies¹ in 14 APAC territories. Interviews were conducted online or face-to-face in English or local languages. Online panels were used in Australia, China, Hong Kong, Indonesia, Japan, South Korea, Malaysia, New Zealand, Philippines, Singapore, Taiwan, Thailand, Vietnam. Interviews were conducted face-to-face in Sri Lanka. Interviews lasted approximately 15 minutes on average.

A hard quota applied to respondents working in government and the public sector at 20% in each territory except China and Vietnam.

Participant profile – region and country, company size, role and sector

<table>
<thead>
<tr>
<th>Number of interviews (region/country)</th>
<th>Number of employees globally</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia 100</td>
<td>Greater than 5000</td>
<td>44</td>
</tr>
<tr>
<td>China 250</td>
<td>1500 – 4999</td>
<td>22</td>
</tr>
<tr>
<td>Hong Kong 93</td>
<td>1,000 – 1,499</td>
<td>15</td>
</tr>
<tr>
<td>Indonesia 100</td>
<td>500 – 999</td>
<td>14</td>
</tr>
<tr>
<td>Japan 95</td>
<td>Less than 500</td>
<td>5</td>
</tr>
<tr>
<td>South Korea 97</td>
<td>Role within organization</td>
<td>%</td>
</tr>
<tr>
<td>Sri Lanka 100</td>
<td>Senior management</td>
<td>19</td>
</tr>
<tr>
<td>Malaysia 100</td>
<td>Middle management</td>
<td>38</td>
</tr>
<tr>
<td>New Zealand 85</td>
<td>Employee</td>
<td>43</td>
</tr>
<tr>
<td>Philippines 101</td>
<td>Industry sector</td>
<td>%</td>
</tr>
<tr>
<td>Singapore 90</td>
<td>Banking/Financial services/Insurance</td>
<td>13</td>
</tr>
<tr>
<td>Taiwan 95</td>
<td>Consumer products/retail/wholesale</td>
<td>9</td>
</tr>
<tr>
<td>Thailand 100</td>
<td>Extractive industries</td>
<td>7</td>
</tr>
<tr>
<td>Vietnam 102</td>
<td>Government &amp; Public sector</td>
<td>11</td>
</tr>
<tr>
<td>Total 1508</td>
<td>Manufacturing</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Pharmaceuticals/Life science</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Power and utilities</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Professional firms and services</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Real estate/Property management</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Technology, communications &amp; entertainment</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Transportation</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>9</td>
</tr>
</tbody>
</table>

¹. Large companies are defined as those with more than 100/150/250/500/1,000 employees locally depending on the territory
Fraud and corruption – driving away talent?
Asia-Pacific Fraud Survey 2015
Contact information

Global Leader/EMEIA Leader
David Stulb  
+44 20 7951 2456

Americas Leader
Brian Loughman  
+1 212 773 5343

Asia-Pacific Leader
Chris Fordham  
+852 2846 9008

Japan Leader
Ken Arahari  
+81 3 3503 3292

Argentina
Andrea Rey  
+54 11 451 52 668

Australia/New Zealand
Rob Locke  
+61 28 2956 335

Brazil
Jose Compagno  
+55 11 2573 3215

Canada
Mike Savage  
+1 416 943 2076

Chile
Ricardo Gameroff  
+56 2 267 6 1414

China
Emmanuel Vignal  
+86 21 2228 5932

Colombia
Liudmila Riano  
+57 1 484 7351

Czech Republic/Slovakia/Slovenia/Serbia/Croatia
Daniel Bican  
+420 225 335 849

Denmark
Torben Lange  
+45 25293184

France
Philippe Hontarrede  
+33 1 46 93 62 10

Germany
Stefan Heilser  
+49 211 9352 11397

Hungary
Ferenc Biro  
+36 1 451 8684

India
Arpinder Singh  
+91 22 6192 0160

Indonesia
Stevanus Sianturi  
+62 21 5289 5000

Ireland
Julie Fenton  
+353 1 221 2321

Italy
Fabrizio Santaloia  
+39 02 8066 9733

Kenya
 Gitahi Gachahi  
+254 20 2715300

Luxembourg
Gerard Zolt  
+35 24 2124 8508

Malaysia
Joyce Lim  
+60 3 749 958 847

Mexico
Ignacio Cortes  
+52 555 2831300

Netherlands/Belgium
Angelique Keijzers  
+31 88 40 71812

Nigeria
Linus Okeke  
+234 1 463 6479 80

Norway
Elisabeth Roscher  
+47 24 002 907

Philippines
Roderick Vega  
+63 2894 8342
<table>
<thead>
<tr>
<th>Region</th>
<th>Name</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poland/Baltic States</td>
<td>Mariusz Witalis</td>
<td>+48 225 577 950</td>
</tr>
<tr>
<td>Portugal</td>
<td>Pedro Cunha</td>
<td>+351 217 912 043</td>
</tr>
<tr>
<td>Romania/Bulgaria</td>
<td>Burcin Atakan</td>
<td>+40 21 402 4056</td>
</tr>
<tr>
<td>Russia/ Commonwealth of Independent States</td>
<td>Greg Crouse</td>
<td>+7 495 755 9968</td>
</tr>
<tr>
<td>Singapore</td>
<td>Reuben Khoo</td>
<td>+65 6309 8099</td>
</tr>
<tr>
<td>South Africa/ Namibia</td>
<td>Charles De Chermont</td>
<td>+27 11 502 0426</td>
</tr>
<tr>
<td>South Korea</td>
<td>Chris Fordham</td>
<td>+852 2846 9008</td>
</tr>
<tr>
<td>Spain</td>
<td>Ricardo Noreña</td>
<td>+34 91 572 5097</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>Averil Ludowyke</td>
<td>+94 11 2463500</td>
</tr>
<tr>
<td>Sweden/Finland</td>
<td>Erik Skoglund</td>
<td>+46 8 520 599 39</td>
</tr>
<tr>
<td>Switzerland</td>
<td>Michael Faske</td>
<td>+41 58 286 3292</td>
</tr>
<tr>
<td>Taiwan</td>
<td>Chester Chu</td>
<td>+88 62 2757 2437</td>
</tr>
<tr>
<td>Thailand</td>
<td>Wilaiporn Ittiwiroon</td>
<td>+66 2264 9090</td>
</tr>
<tr>
<td>Turkey/Greece</td>
<td>Dilek Çilingir</td>
<td>+90 212 368 5172</td>
</tr>
<tr>
<td>UK</td>
<td>John Smart</td>
<td>+44 20 7951 3401</td>
</tr>
<tr>
<td>US</td>
<td>Brian Loughman</td>
<td>+1 212 773 5343</td>
</tr>
<tr>
<td>Vietnam</td>
<td>Saman Bandara</td>
<td>+84 4 3831 5100</td>
</tr>
<tr>
<td>Zimbabwe</td>
<td>David Gwande</td>
<td>+263 4 750979</td>
</tr>
</tbody>
</table>
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY’s Fraud Investigation & Dispute Services
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter the industry sector. With our more than 3,400 fraud investigation and dispute professionals around the world, we assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. And we work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide.

© 2015 EYGM Limited.
All Rights Reserved.
APAC no: 00000296
BACS 1002178
ED 0517

In line with EY’s commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com