FINANCIAL CRIME STRATEGY

Tackling a Trillion-dollar Issue

BY
TIM PHILLIPPS

In March 2014, Deloitte held Financial Crime Strategy conferences in Singapore, Jakarta and Hong Kong. Choosing Singapore as the first location globally to launch the programme, the three-city symposium series, sponsored by IBM, gave delegates – senior decision-makers within the risk compliance and legal functions – an overview of the financial crime challenges they face, and the steps needed to successfully deal with those challenges.

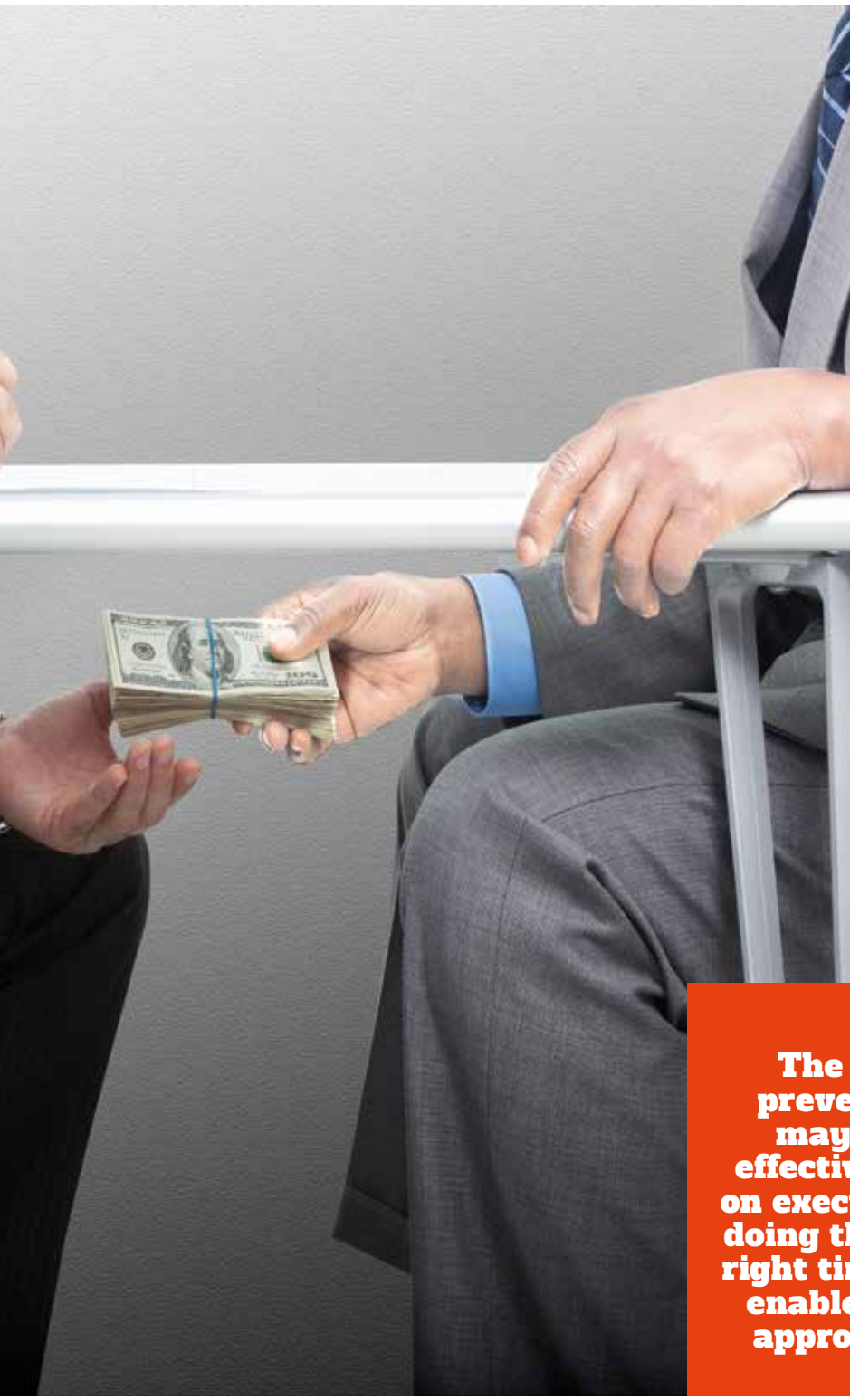
Delegates heard presentations on the regulatory environment, industry trends, analytics, technology and target operating models, and were asked polling questions throughout the day. After lunch, delegates attended interactive breakout sessions. During these sessions, they spent 15 minutes with four sets of facilitators. Discussion was focused on key financial crime strategy themes – barriers, drivers, risks and analytics. The objective of the sessions was to enable participants to share their views on the main issues they are encountering in financial crime.

It became clear that financial crime is an ever-present threat for financial services organisations. The value of what criminals take is only part of the cost – there are also penalties, civil judgements, and the cost of conducting investigations... and that's not yet counting the massive costs associated with reputation.

Corporate officers feel a perfect storm of pressure. Bribery, fraud, and cyber crime keep getting more sophisticated. Regulatory agencies demand more accountability. And as business embraces globalisation, it encounters nuanced new cultural and legal challenges. A fragmented approach isn't enough, and neither is a purely reactive one.

Despite these challenges, many current financial institution approaches to financial crime often remain a patchwork of fragmented, inefficient and ineffective efforts designed around a discrete set of compliance chores. Simply stated, financial services companies can no longer take the "bare minimum" approach to compliance. They need to invest in creating an integrated approach to the risk of financial crime to protect themselves not only from serious financial repercussions, but damage to their brand reputation as well.

PHOTO CORBIS



MONEY, THE ROOT OF ALL EVIL?

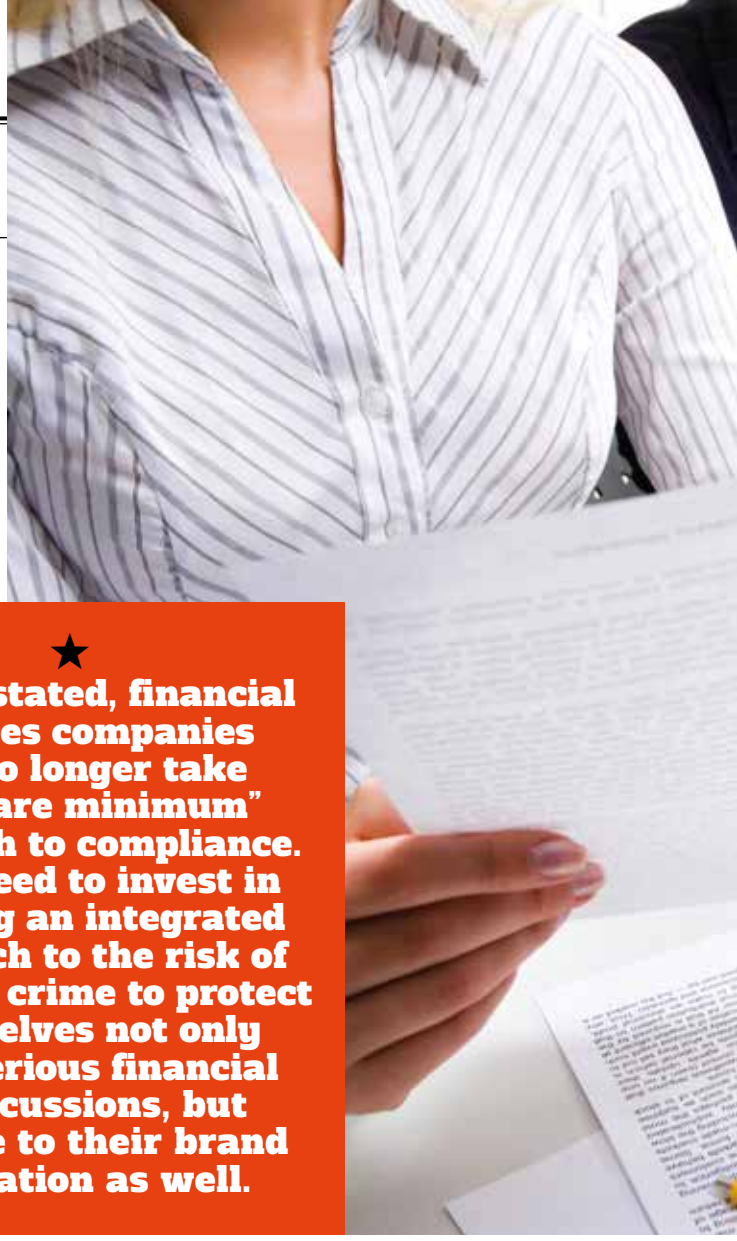
Financial crime is a well-known and widespread problem that impacts brand value and reputation, goodwill, and revenue of many organisations. For example, money laundering alone is estimated to be in the region of USD2 trillion per annum. In addition to the risk of losses from the financial crime itself, companies also face spiralling costs in related areas. Compliance with increasing regulation, ongoing crime detection efforts, internal investigations of potential wrongdoing, external enforcement actions and any associated fines and penalties, class action lawsuits, and other litigation are among the factors driving up both the costs and risks associated with financial crime. In order to effectively detect, assess, prevent, and respond to financial crime, organisations should consider a more strategic and holistic risk management approach.

So what exactly do we mean by financial crime? From fraud to electronic crime, from money laundering to bribery and corruption, from market abuse and insider dealing to sanctions – all of these forms of financial crime are on the rise and share a common denominator: money.

Companies are managing the risks associated with financial crime in a variety of ways. Compliance-based approaches addressing particular

★

The infrastructure to prevent financial crime may be sound, but its effectiveness still depends on execution, on individuals doing the right thing at the right time – culture is what enables and drives those appropriate behaviours.



risks in a siloed or piecemeal fashion are giving way to holistic approaches that look at many types of financial crime risk across the organisation. Regulators expect to see this risk-based approach, yet still expect an overall compliance strategy. Regulators are looking for someone such as a Chief Compliance Officer or Chief Legal Officer to have overarching responsibility. Overall, the trend is toward a broader risk-based approach with shared responsibility by management, staff, the Board of Directors, and internal audit. Accomplishing this transition typically involves a focused change management effort for the organisation.

With this in mind, why do companies' compliance, anti-fraud, anti-money laundering, and similar programmes fail? Failure to prevent or detect issues is often not because the programmes or controls themselves are lacking. More often, it's a failure of culture and a lack of effective change management. For example, senior leaders may not be setting a strong or consistent tone at the top about acceptable and unacceptable behaviours. Or perhaps there isn't enough attention paid to getting the buy-in from the lines of business for new policies or processes. Or staff training and awareness efforts may be lacking. The infrastructure to prevent financial crime may be sound, but its effectiveness still depends on execution, on individuals doing the right thing at the right time – culture is what enables and drives those appropriate behaviours.

It's clear that technology also plays a critical part in combating financial crime. Technology tools can give organisations a more holistic view of their data, highlight potential areas of risk and allow them to be more focused or targeted in their efforts to combat financial crime. Advanced analytics may help companies be more predictive

★

Simply stated, financial services companies can no longer take the "bare minimum" approach to compliance. They need to invest in creating an integrated approach to the risk of financial crime to protect themselves not only from serious financial repercussions, but damage to their brand reputation as well.

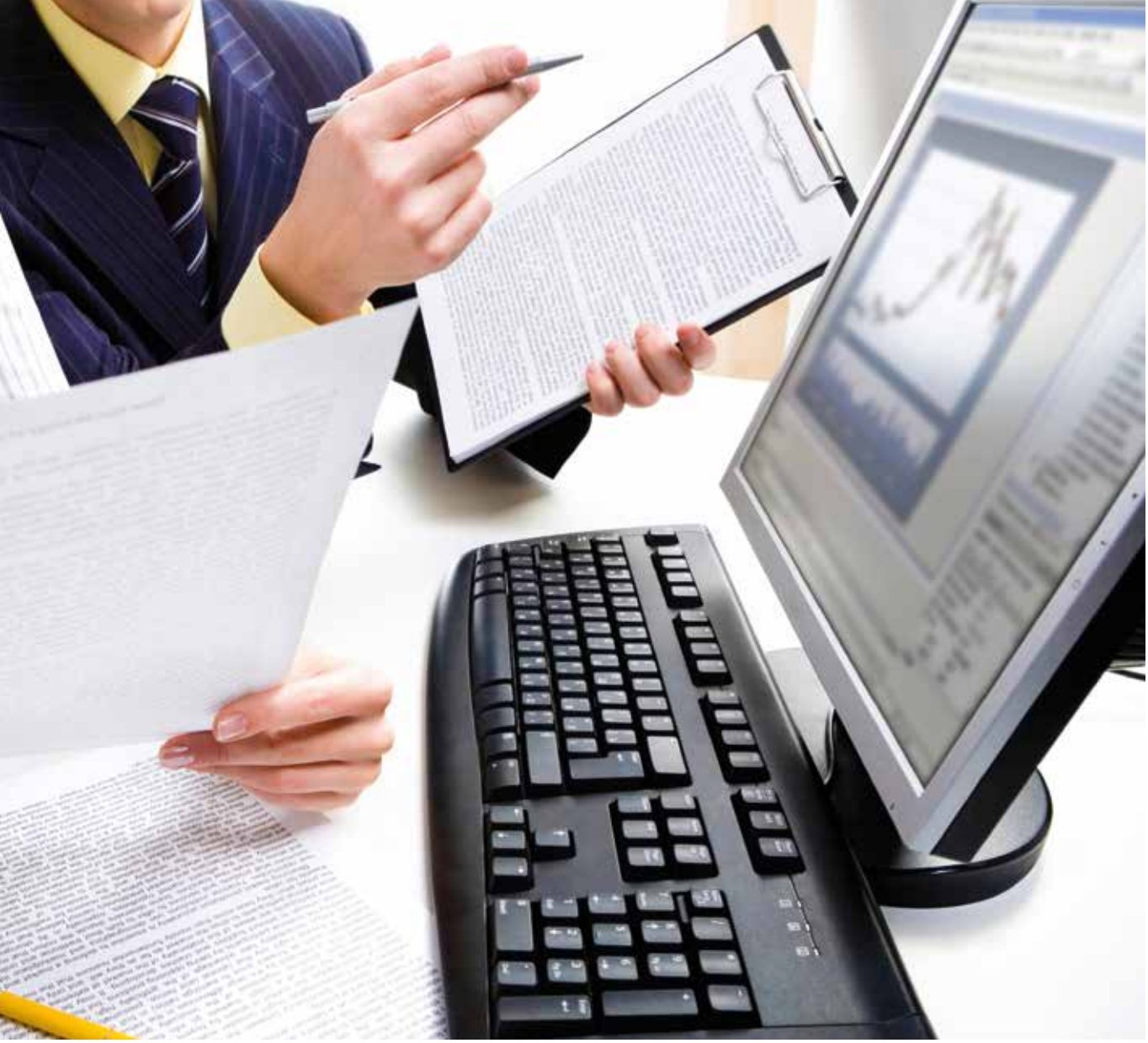
KEY OBSERVATIONS

Delegates clearly recognised the need to deal with financial crime holistically and identified the following issues as critical to their financial crime strategy formulations:

- The cost, both financial and reputation, of non-compliance is increasing.
- A holistic change management process is an important factor in an effective financial crime strategy.
- With ever-increasing and more complex threats, financial crime benchmarking should be comprehensive and conducted regularly.
- There are increasing regulatory requirements from local, regional and global stakeholders.
- There is an increasing need for an analytical understanding of financial crime.
- The complexity of implementing and ongoing management of financial crime analysis and reporting is becoming a major issue for organisations.
- Technology is key in highlighting potential areas of risk and allowing them to be more focused or targeted in their efforts to combat financial crime.
- Organisations' financial crime approaches are constantly changing and evolving to deal with new issues.

Source: Financial Crime Strategy Report, Deloitte

PHOTO ISTOCKPHOTO



in identifying trends and patterns indicative of financial crime risk that are not otherwise easily discernable. Overall, the emphasis today is on prevention and/or early detection; leveraging technology and analytics to proactively identify issues or potential issues before they turn into front-page news.

DIFFERENT LOCATIONS, DIFFERENT CHALLENGES

Throughout the conference, the polling responses and breakout sessions clearly indicated that financial crime is a key issue for organisations. For example, Singapore and Hong Kong respondents both agreed that their organisation's operational structure posed the greatest financial crime challenge while nearly half of Jakarta delegates noted that their greatest challenge is related to external change such as economic, geopolitical and market drivers.

Regulatory change is also clearly a key concern for industry – the vast majority of delegates agreed that regulatory change will increase in Asia in the coming five years. Interestingly, not one delegate in Jakarta believed that regulatory change will reduce in the coming years. Not surprisingly, the majority of respondents noted that their organisation addressed regulatory change in both a tactical and strategic manner. Jakarta organisations appear to possess more of a calculated approach, with 26% of respondents advising that they respond strategically.

In closing the Asia-Pacific events, delegates noted that it is crucial to implement an integrated approach which enables firms to seek out additional synergies between financial crime intelligence and customer intelligence, thereby creating opportunities to improve customer service and add more business value. The delegates clearly agreed that an integrated approach is required as polling results indicated that they expect to react to regulatory, organisational and cultural financial crime changes in the months and years ahead. ISCA

The Deloitte Asia-Pacific Financial Crime Strategy Report is available at www.deloitte.com/view/en_SG/sg/services/financial-advisory/forensic

Tim Phillipps is Global Leader – Deloitte Forensic.