Donald Joshua Jaganathan: Enterprise risk management - harnessing disruption

Opening remarks by Mr Donald Joshua Jaganathan, Assistant Governor of the Central Bank of Malaysia (Bank Negara Malaysia), at the Institute of Enterprise Risk Practitioners (IERP) Annual Conference 2017 "Enterprise Risk Management – Harnessing Disruption", Kuala Lumpur, 23 May 2017

* * *

It is my pleasure to have the honour of addressing you this morning. I would first like to take this opportunity to congratulate the organisers for successfully gathering an array of distinguished speakers to share their broad-ranging and invaluable experiences. The breadth of the programme over the next few days reflects how vast the area of Enterprise Risk Management (ERM) has evolved, and how much there is for risk managers today to discover, learn and master. In my speech this morning, please allow me to share my thoughts on risk management, amid the so-called "age of disruption".

Technology and risk management

Amongst all 'disruptions' witnessed thus far, perhaps none have been as forceful and impactful as technological disruptions. Take the smartphone, its use has permeated almost every aspect of our daily lives and has become almost like another limb for some of us. I'm no longer woken up by an alarm clock, nor do I read the papers on "paper" or take photos on a camera. In the palm of my hand I hold a music player, internet browser, GPS navigator, torchlight, and compass, even a wallet in more and more places. With a couple of taps I can hail a cab, and monitor my home CCTV, or buy any number of goods from across the world, which might, in the not too distant future, be delivered to my doorstep by a flying drone.

Given how extensively technology has altered our world today, being technology savvy has become a crucial requirement for risk managers today. In what seems like a blink of an eye, companies like *Uber*, *Waze* and *Airbnb* which barely existed a decade ago have become household names. Now valued in the billions, they are a source of income for thousands of people across the globe, and are shaping our modern economy in a myriad of ways. Technological savviness is crucial for two reasons. First, technology can be harnessed to improve business operations and enhance risk management. Secondly, it allows us to quickly identify and respond to new sources of risks emanating from technological developments.

The potential of technology in risk management is vast, not only for the automation of tasks, but increasingly as a tool for making business decisions as well. The application of big data analytics and artificial intelligence to assess and predict human behaviour, for instance, can provide great value to businesses in terms of reducing risks. In the motor insurance sector for example, *General Motors Assurance* in the US has been utilising mileage and driving behaviours captured through in-vehicle telecommunication devices. *Telematics*,as this approach is called, enables the incorporation of personalised information distinct to the policyholder in setting insurance premium prices and rewards those who continuously maintain good driving standards – a win-win situation for both the insurers who mitigate their underwriting risk and consumers who benefit from lower premiums.

Technology has also advanced to a level where machines' capabilities extend beyond simple tasks, but also able to carry out complicated tasks by professionals more quickly and efficiently. A bank in the US, for example, has created a machine-learning programme to sieve through and review legal contracts in mere seconds, saving 360,000 of labour hours which are better spent on more productive tasks. It is an ideal worker – having a low margin for error which minimises the occurrence of costly mistakes, and better yet, never gets ill or asks for leave. Of course,

investments in technology may be expensive and returns may not be immediate. It is, nevertheless, not a choice and it is crucial to start early. Not innovating along with the latest technology should not only be seen as lost opportunities, but also lead to risk of your business being rendered obsolete.

Business transactions and financial services are becoming more digitised and reliant on the internet. Alongside this, the extent of technology risks and the level of sophistication of cyber-attacks are rapidly expanding. There is a need for risk managers to be quick in identifying and responding to cyber risks. With increasing dependence on information technology, institutions are faced with numerous threats such as distributed denial of service, malicious hacking and virus attacks which affect vital services provided to customers. Barely a week ago, the vulnerability of major organisations to such attacks was laid bare when a massive "ransomware" virus hit up to 300,000 computers across 150 countries including Malaysia. Judging from its name, the "*WannaCry*" virus clearly achieved its aim as users found themselves locked out from their computers and their data held at ransom. A host of organisations were left reeling in the wake of these cyber extortion attacks, including the Russian interior ministry, delivery and shipping giant *FedEx* and the UK's *National Health Service* where some hospitals were unable to perform operations, putting patients' lives at stake.

There is also the danger of phishing and stealing of confidential customer data which could destroy the trust placed on your company. *Yahoo!*, one of the internet's top sites with a billion monthly users, suffered a massive security breach in 2014 when hackers stole the personal details of at least one billion user accounts. The implications are far-reaching as a stolen digital identity makes us vulnerable to manipulation and undermines the safety of, not just ourselves, but also the ones we love. Bank accounts, social media profiles and even medical information can be abused to put us and our family in harm's way. In the months following the hacking revelations, more than five billion dollars was wiped off *Yahoo's* market capitalisation. This was not an isolated incident and sadly, many more companies could fall victim to cyber-attacks. Last month, a report by cyber security consultancy *CGI Group* and *Oxford Economics* estimated that severe cyber-attacks have cost shareholders losses exceeding £42 billionsince 2013 as a result of falling share prices. And this does not even include the damage from lost consumer confidence which is not easily rebuilt.

These cases of cyber-attacks serve as a wake-up call to risk managers, as lagging behind in the latest technology is no longer an option. Missing the boat can bring dire consequences, not only tobusinesses but also to the overall safety and soundness of the socio-economic and financial system. Recognising this, technology risk has been one of the top priorities of Bank Negara. Allow me to share some of the Bank's efforts thus far:

a. In March this year, Bank Negara began testing current institutional capabilities in managing cyber threats. Malaysian banks were required to participate in the National Cyber Drill exercise, and the results showed that the millions invested on modern security countermeasures have paid off, with our banks remaining resilient. Notwithstanding this however, the key message is that we must be vigilant. We must be alert. We must be prepared.

b. A key tool in identifying IT security vulnerabilities is the practice of penetration testing or "pen-testing", where a simulated attack is carried out on IT systems by "ethical hackers". As part of the efforts to improve the standard of pen-testing in Malaysia, Bank Negara Malaysia facilitated the formation of a task force last October, to set up a Malaysia chapter of the UK-based *Council of Registered Ethical Security Testers* or *CREST*, which will serve as a certification body for ethical hackers. We believe that this is a good platform to grow domestic talent in this area and promote international best practices in penetration testing.

c. The Bank has also launched the *Operational Risk Integrated Online Network* or commonly known in the industry as the *ORION* system, to enhance the standard of operational risk

management in the financial sector. *ORION* is a risk surveillance system that consolidates information on operational risk incidences, including cyber-attacks. The system will strengthen the Bank's ability to perform system-wide monitoring and early detection of developing trends in cyber-attacks and frauds within the financial sector.

Moving forward, Bank Negara Malaysia is looking to address identified gaps in technology risk management practices within the financial sector. As part of this effort, the Bank is in the midst of conducting a comprehensive review of existing technology risk guidelines, including enhancing the expectations for the board and senior management to play a more active role in managing technology risk, and enhancing the resilience of IT infrastructures such as data centres.

In today's world where there is increasing uncertainty of what the future may hold, it is no longer possible for risk managers to rely solely on historical trends. The 2008 subprime crisis is a textbook example of how backward-looking data is not a good indicator for the future economic environment. Hence, organisations need to be pragmatic and shift towards more forward-looking and proactive risk identification, assessment and management. In a recent financial industry survey conducted by the Bank to gauge the top operational risks among financial institutions, it is evident that most financial institutions are still focused only on "typical" risks such as card fraud and operational errors, rather than proactively anticipating and preparing against emerging risks. This has to change. In this regard, the Bank highly encourages pre-emptive and forward-looking risk management practices such as scenario analysis to anticipate the potential impact of future threats to an organisation and provide sufficient time for remedial actions to be taken.

Incorporating culture into risk management

Let me now move on to another element that a good risk manager cannot ignore, which is the importance of incorporating culture into enterprise risk management. At the heart of every corporate scandal is the failure of the people at different levels of the institution to uphold the highest standards of ethical behaviour and integrity. This is the reason why organisations need to do more than just comply with rules and regulations. The accounting scandal at a major Japanese conglomerate recently, illustrates this point. The company was once seen as exemplary in corporate governance. Such was its reputation that it frequently appeared as a case study in books on governance. We now know that the truth was quite the opposite, with findings that top executives were involved in accounting malpractices over the past seven years. The reality was that while its governance structure looked good on paper, its execution had been marred by its organisational culture. According to the investigation report, top management was systematically involved in the inflation of numbers and drove the company into a place where profits were paramount. The number of similar cases reported in the media highlights how detrimental poor internal culture can be for any organisation, not only in terms of financial losses and the imposition of hefty regulatory fines, but also a potential permanent blow to the company's reputation.

Risk culture, in my view, is a key factor in determining the robustness and effectiveness of risk management in an institution. At Bank Negara, there has also been increasing focus on preserving the integrity and trust in our financial sector. Last year, the Bank published the enhanced *Corporate Governance* framework for financial institutions in Malaysia. The enhancements relate to expectations for the board and senior management to set the right "tone from the top" and play a more critical role in shaping the core values and culture of the institution. This includes expanded requirements on compensation practices and disclosures to strengthen market discipline, as well as putting in place a transparent whistleblowing policy that enables the escalation of concerns without the risk of reprisal.

More recently in April, the Bank published the *Code of Conduct for the Malaysian Wholesale Financial Markets* to promote high standards of conduct and transparency in the domestic wholesale financial markets. The code is a binding obligation and it sets out the Bank's

expectations for market participants to adhere to professional and ethical standards of conduct. The Bank views this standard as critical and timely in light of the incidences of ringgit-rate fixing misconduct and also involvement in the opaque NDF market.

Another important aspect of preserving the integrity in the industry is by maintaining strict membership requirements for all participants. As an industry riding on trust as the main vehicle for business, the financial sector cannot afford to be tainted by the actions of a few bad apples. Any unscrupulous behaviour exhibited by a player should not be tolerated and be weeded out immediately from the industry. To protect the financial ecosystem, each organisation has the responsibility to investigate any misconduct and record the outcomes to allow other institutions in the market to make informed decisions on the ability of a person to serve with professionalism and integrity. In this regard, the Bank is currently pursuing an initiative that will mandate the sharing of employment references with future employers to mitigate the problem of 'rolling bad apples' within the Malaysian financial industry.

Specific and rules-based regulations, while able to lead institutions in the right direction, do not guarantee the internalisation of such values within bankers nor are they dynamic enough to catch up with new ways of breaching ethics. Therefore, the Bank will also be expanding its supervisory focus on financial institutions beyond balance sheet ratios, and incorporating organisational culture in our radar such as tone from the top, echo from below, accountability, communication, remuneration and performance management. This is a challenging but necessary task that requires creativity in exploring unconventional supervisory approaches including interviews and questionnaires for employees of financial institutions among others..

Risk management as part of business strategy

Finally, risk managers must move away from merely compliance and loss prevention. Risk managers must reposition themselves to be more engaged in strategic business decisions within their respective organisations. Chief Risk Officers (CROs) must have a broad and independent view of the organisation, with an ability to anticipate potential disruptions and to influence decision-making. However, according to a global survey conducted by *PwC* last year, only 1/3 of risk officers view themselves as part of the business. Especially now in the age of disruption, risk managers should not view themselves as mere compliance officers or the mundane department that says 'no' to exciting business opportunities. Instead, risk managers need to also think in terms of finding the right risk-return trade-off. Risk management must go beyond the prevention of losses and play an active role in driving business sustainability and enhancing shareholder value.

Given the importance of enterprise risk management, efforts need to be directed to give prominence to this function. It is time for the stature of risk functions to be elevated. Professional bodies like the IERP play a crucial role in stewarding this transformation by equipping risk management experts and raising their credibility through branding and professional qualifications. Events like this conference can help propel the risk management agenda forward. However, beyond technical competency, risk managers increasingly require confidence and communication skills to be the resounding voice in promoting risk culture. Risk managers need to have a seat at the executive table and play a role in shaping the risk profile and risk culture of your organisations. A study conducted by *Harvard Business School* highlights how leadership and communication by risk managers can influence the significance of their role within organisations. As expected, the study found that risk managers that proactively sought opportunities to raise their visibility were able to assert risk management perspectives and were better able to position themselves as critical voices within organisations.

Ladies and gentlemen

The task of a risk manager in an organisation is like that of a ship navigator. As you work closely

with your captain to navigate your ship across unknown waters, your job is to ensure you get your ship to its destination in one piece. You never know what hazards may lie ahead but whether it be foul weather, rough seas or hostile forces, you stand ever ready to face them. The things that set great risk managers apart, like great navigators, are their ability to work with their captain and crew as a unit, their skills at employing the tools at their disposal to deal with risks at hand, and their attention to their surroundings for signs of impending threats.

With that, I wish you all a smooth-sailing journey ahead and a productive and fruitful conference over the next two days. Thank you.