COMMERCIAL CRIME International

September 2018

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

Alerting business to the threat from fraud and corporate crime, and its prevention

'Keep on top of the ever-changing governance landscape'

THE regulatory landscape is evolving and changing, and it is now more important than before that companies comply with proper governance – ignore at your peril!

Organisations must also take into account 'new' social pressures which can have a huge impact on them and which will involve widening their current governance procedures and policies.

David Hughes, Partner at Stewarts Law LLP made these observations in his keynote speech at the International Financial Crime and Money Laundering Forum organised by ICC Financial Investigation Bureau (FIB) in Kuala Lumpur, Malaysia in July.

In a reasoned and fascinating review titled *Governance in the new era – embracing change, challenges and opportunities*, he spoke about how the loss of reputation for non-compliance can be extremely high for businesses and reminded the audience that negligence can result in not just civil, but criminal penalties as well.

"Good governance is essential to a business' success and longevity, but it is also an evolving concept. What might have been good governance 10 years ago is not acceptable now; business must evolve with changing demands or wither. It is not sufficient to pay lip-service to policies or procedures. It is necessary to stress-test them for effectiveness on a regular basis," Hughes said.

Hughes framed his presentation on five main areas – money laundering, bribery and corruption, sanctions, equality and diversity and responsible accounting – drawing from recent and historical examples on how organisations suffered, at best, a costly reputational misstep and, at worst, a reputational and financial disaster.

These include;

- an attempt to trivialise the Black Lives Matter movement by Pepsi last year
- the forcible removal of a passenger from United Airlines
- the collapse of outsourcing giant Carillion
- the stripping of Uber's London licence
- fines meted to Facebook for its part in the Cambridge Analytica scandal. (WhatsApp and Talk Talk suffered similar fates)
- the BCCI scandal in the early 1990s in the wake of the CIA uncovering massive money laundering activities
- the exposure of lax anti-money laundering procedures at HSBC, which resulted in a £1.2bn fine and the bank entering a five-year deferred prosecution agreement (DPA)
- the corruption and bribery scandal that hit Rolls Royce resulting in an eye watering fine of £671 million, the largest criminal penalty in British history
- in 2012, Standard Chartered Bank was accused by New York's Department of Financial Services of helping the Iranian government circumvent US sanctions in the amount of £191.8 billion over 10 years
- the scandal that marked the end of Enron and the end of Arthur Andersen
- sexual offences in the workplace, notably the much-publicised fall of Harvey Weinstein and a culture of silence whereby such behaviour is normalised and remained unaddressed due to toxic internal cultures, differing and evolving attitudes as to what is and is not acceptable.

According to Hughes, even if a business survives financial upheaval, it may not survive the reputational consequences, as seen in some of the aforementioned examples. These could include loss of shareholder faith, loss of public faith, removal of

Continued on page 2/

In This Issue of CCI

WHISTLEBLOWING
US proposes changes to payouts 3
FRAUD
Director jailed invoicing fraud 4
MONEY LAUNDERING
Skill sets of professional launderers 5
Solicitors see rise in ML reports 6
CORRUPTION & BRIBERY
Malaysia gets tough on corruption as 1MDB probe gathers pace 7
CYBERCRIME
Commoditisation of phishing kits fuel attacks 10
Singapore financial firms must tighten checks 11

from page 1 - how to keep on top of good governance

practicing licences and blacklisting in respect of public tenders are all possible fates for a business that does not maintain acceptable governance standards.

Hughes said that money laundering, bribery and corruption, international sanctions and corporate accounting are issues requiring constant monitoring and attention. He said business must embrace technological innovation in conjunction with the continued use of compliance procedures in order to keep up with the constantly changing landscape.

"Equality and diversity and responsible business management continue to be relevant to wider governance concerns and issues remain in respect of effective policies that still need to be resolved. Positive action by individual companies will, at best, form part of a joint action to affect progress and, at least, prevent breaches. Those who embrace change will thrive; those who do not will wither," he cautioned.

Here we summarise the key five areas touched upon by Hughes.

Money laundering

Good governance demands that your organisation has in place systems that enable you to comply with your legal obligations. It is not just about avoiding fines. Or repaying huge sums to victims of control weaknesses. It is about avoiding criminal consequences.

It is about reputational risk. It is about establishing a culture focused on avoiding regulatory breaches and everything that entails. Evolving areas of concern include money laundering through capital markets and a growing number of criminals laundering money through crypto-currencies. In summary, good governance demands that firms embrace new technologies able to better detect patterns and sources of transactions, to ensure that they do not fall foul of dirty money.

Bribery and corruption

It is clear that businesses must do more by way of compliance with anti-bribery legislation. The Rolls Royce case illustrates the current global drive towards encouragement of self-reporting in return for the benefit of relative leniency; France has introduced the use of DPAs and Australia is now following suit.

However, prevention is better than cure; Rolls Royce could afford to pay this fine, others may not be so lucky. Multi-jurisdictional businesses face the additional difficulty of dealing with several enforcement agencies at once, which may have implications on the penalties imposed and will certainly make the investigations more complex. From a governance perspective it is far better to have effective compliance safe guards in place and avoid the need to self-report altogether.

Sanctions

The current political uncertainties – Brexit, Trump's reneging on the Iran deal, Trump's discussions with North Korea, growing tensions between the West and Russia – mean that international firms operating in jurisdictions where sanctions are in place must keep abreast of developments so that they remain proactive rather than reactive.

As with money laundering, sanctions compliance raises concerns as to who your client is. Never before has 'Know Your Client' been more important. You need to consider new technology that can make this process more efficient and provide greater transparency. The ability to collect data on a daily basis will feed into the monitoring you need to have in place.

Equality, Diversity and Discrimination

From a governance perspective, sexual harassment has no place in the work place. While it is the individual that bears the brunt of the reputational costs of a sexual harrasment allegation, a firm that is revealed to foster a culture of harassment will be treated unkindly in the public domain in the post-Me Too era. Equality and diversity policies are essential. This policy needs to be made effective and enforced.

There needs to be change in the Board Room and a continued thrust towards positive action and a sustain-able cultural change within business in order to begin to reap the benefits of an additional work force that we are still collectively underusing and undervaluing.

Responsible accounting

While the Enron scandal is almost 20 years old, the lessons to be learned from it remain as pertinent today, not least because they have not necessarily been learned by some businesses, or by their auditors, who continue to tread the precarious tightrope of audit independence versus company growth.

Hughes says that at the end of the day it boils down to the 3 C's: **Culture, Culture, Culture**. Culture filters from the top down, not from the bottom up. Governance is not simply a matter of pointing to the policies and procedures in place; they must be effectively implemented and those in control must lead from the front.

"Where directors do not set good governance standards they can expect internal culture to follow in kind. Where corrupt procedures become normalised the risk of rogue traders (think Barings) increases, as does the fear of blowing the whistle.

"We must not only keep on top of good governance but espouse it in order to keep businesses safe and profitable," he said.

US proposes changes to payouts

THE Securities and Exchange Commission in the US has voted to propose amendments to the rules governing its whistleblower program, which includes considerations for small and exceedingly large awards.

SEC said for potential awards that could yield a payout of $2 million or less to a whistleblower, the proposed rules would authorise the Commission to adjust the award percentage upward under certain circumstances.

SEC said the potential increase would be to an amount that it determines more appropriately achieves the program's objectives of "rewarding meritorious whistleblowers and sufficiently incentivising future whistleblowers who might otherwise be concerned about the low dollar amount of a potential award."

It added that any upward adjustment would be subject to the 30 percent statutory maximum.

Equally, SEC is proposing that for potential awards of $100 million, adjustments can be made that the payout (subject to the 10 percent statutory minimum) does not exceed an amount that is reasonably necessary to reward the whistleblower and to incentivise other similarly situated whistleblowers.

SEC said however, in no event would the award be adjusted below $30 million.

Currently, SEC's whistleblower rules do not expressly permit the Commission to consider whether a relatively small or exceedingly large potential payout is appropriate to advance the program's goals of rewarding whistleblowers and incentivising future whistleblowers.

SECs whistleblower program was established in 2010 to incentivise individuals to report high-quality tips to the Commission and help the agency detect wrongdoing and better protect investors and the marketplace.

Original information provided by whistleblowers has led to enforcement actions in which the Commission has ordered over $1.4 billion in financial remedies, including more than $740 million in disgorgement of ill-gotten gains and interest, the majority of which has been, or is scheduled to be, returned to harmed investors.

The Commodity Futures Trading Commission (CFTC) last month announced multiple whistleblower awards totalling more than $45 million.

In July, the CFTC announced an award of approximately $30 million to one whistleblower and the first award was made by the program to a whistleblower living in a foreign country.

A repeat offender who created fake identification documents and stole business current account numbers has been sentenced to 65 months in prison for his latest string of frauds.

He pleaded guilty to stealing more than US$287,000 from banks and businesses in January 2018.

The offender and his co-conspirators stole personally identifying information and created fake IDs in the victim names. They also stole business current account numbers.

Using the fake IDs and forged cheques, they would make bank deposits and withdraw cash before the financial institution discovered the fraud. The conspirators also purchased mobile phones and opened lines of credit in the stolen identities. In 2009, the man was sentenced to 75 months in prison for a fraud totalling more than US$564,000.

Ghost brokers went all out to appear authentic

THREE men from London, UK orchestrated an elaborate ghost broking scheme taking profits from their unsuspecting victims by selling them fraudulent insurance policies.

The trio operated under a limited company called AHD Solutions between June 2012 and August 2013 and went to great lengths to seem legitimate, conducting the scam out of a real office and even setting up a website which they used to specifically target minicab drivers.

The fraudsters even went so far as to employ someone on work experience at the fraudulent company, who had no knowledge of the scam. Their ploy was uncovered by the Insurance Fraud Bureau (IFB) and the Metropolitan Police Service.

As part of the scam, AHD would advertise Hire and Reward policies and then add the minicab vehicle onto a trade policy. This ensured that the cars would not flag up as uninsured to police and other agencies, but still left the minicab uninsured for Hire and Reward. They would also issue seemingly legitimate policy documents.

In order to appear authentic, AHD Solutions were also using the name of insurance company, esure, on their website. However, esure became aware of this copyright infringement and took legal action to prevent misuse of its brand in April 2013, going on to collaborate with the MPS and IFB in the wider investigation that followed.

As part of the investigation, IFB were able to link nine trade policies and 14 personal lines policies to the scammers, identifying 65 vehicles which they believed to be private hire vehicles with invalid policies.

Trading firm director sentenced for invoicing fraud

HONG KONG's Independent Commission Against Corruption (ICAC) has charged and taken to court a trading company director accused of defrauding a bank of export invoice financing loans totalling about HK$13 million by using false commercial invoices.

The defendant was the director-cum-shareholder of D.D. Industries Limited (DDIL), which was engaged in plastic home accessories business.

He was able to convince Standard Chartered Bank (Hong Kong) Limited (SCB) to grant his company the trade credit facility.

Between December 5, 2013 and January 29, 2015, he submitted 18 export invoice financing loan applications to SCB.

To support the applications, he attached 38 commercial invoices of DDIL purportedly issued to four companies for sales and delivery of goods respectively.

In the belief that the transactions and/or the contents of the 38 invoices were genuine and DDIL was awaiting payments from the buyers, SCB approved the 18 applications and released loan payments totalling about HK$13 million to the DDIL account maintained with the bank.

Following ICAC intervention and enquiries, it was revealed that the four companies had never placed the orders with DDIL pursuant to the 38 invoices, and had never received the invoices from DDIL.

During the trial the court was told that had SCB known that the invoices submitted by DDIL in support of the applications were bogus or contained any false information, the bank would not have processed the applications and released the loan payments to the company.

He was sentenced to 12 months' imprisonment.

UK man conned investors out of £14m

A man in the UK defrauded investors out of £14.5 million in a Ponzi scheme, and used his ill-gotten gains to fund his gambling habit, as well as pay for holidays abroad and his children's school fees.

The investments made by his victims varied between £20,000 and £750,000 per person.

An investigation by the City of London Police's Fraud Squad found that between 2005 and 2017, he had been running a Ponzi scheme through wealth management company HBFS Financial Services Limited (HBFS), of which he was managing director.

The case was referred to the City of London Police by the Financial Conduct Authority (FCA) who became suspicious of the HBFS bank accounts.

The fraud ran in parallel with legitimate HBFS business, with the man using the company's name as a means to defraud victims out of vast sums of money. Fifty-five victims invested a total of £14,545,494.48.

The fraudster would convince victims, some of whom he knew personally as friends, that their funds were being held in a high interest bank account which were offering between four and eight percent interest annually.

He told them that they could obtain interest each month and they were advised that their money was locked in for varying amounts of time, between three months and five years.

The investigation found that victims were transferring large sums of money into the HBFS business accounts, under the impression that they were investing in high interest accounts.

However, it was found that large sums of money were being transferred into David's personal bank accounts for his own use as well as being used to pay other investors their "monthly interest".

A review of the perpetrator's personal bank accounts showed that once he had received transfers from HBFS related accounts, he used this money to fund his gambling habit, as well as for paying his children's school fees and holidays abroad.

Between January 2005 and November 2017, he spent £15.6 million on gambling websites and £240,000 in one day alone.

Victims were provided with forged bank documents which supposedly confirmed that the investments had been made and that interest was being accrued each month.

He was sentenced to six years in prison after pleading guilty to the fraud.

FATF reveals 'skill sets' of professional money launderers

A report published by the Financial Action Task Force (FATF) provides examples of financial enterprises that have been acquired by criminal enterprises or co-opted to facilitate money laundering.

The report identifies key 'skill sets' and characteristics of professional money launderers (PMLs) and the network of various parties working together to carry out such activities.

FATF said effective dismantling of PMLs requires focused intelligence collection and investigation of the laundering activities of those groups.

It said many countries continue to limit their investigations to self-launderers: criminals who launder the proceeds of drug trafficking, fraud, tax evasion, human trafficking or other criminality.

"While this may address in-house or self-laundering, it does not impact on those specialised in providing criminals with money laundering services.

"PMLs, professional money laundering organisations and professional money laundering networks can survive law enforcement interdiction against any of its criminal or organised crime group clients, while still standing ready to support the next criminal clientele," FATF said.

The report looks at the techniques and tools used by professional money launderers, to help countries identify and dismantle them.

It has revealed that many countries are not sufficiently investigating and prosecuting complex and third-party money laundering.

The dismantling of PMLs, can impact the operations of their criminal clients, and can be an effective intervention strategy against numerous criminal targets, FATF said.

The report identifies the key 'skill sets' and characteristics of the individual professional money launderer, the professional money laundering organisation and the professional money laundering network of associates and contacts that work together to facilitate money laundering.

It also identifies the various roles and functions that are necessary to operate a professional money laundering 'business' and provides a detailed explanation of the roles performed by PMLs to enable authorities to identify and understand how they operate.

This report also provides recent examples of financial enterprises that have been acquired by criminal enterprises or co-opted to facilitate ML. Using the case studies collected, it identifies a range of different money laundering organisations and networks, from money transport and cash controller networks to proxy networks.

FATF said, "Professional money launderers use a variety of money laundering tools and techniques such as trade-based money laundering, account management mechanisms and underground banking and alternative banking platforms. To lend a veneer of legitimacy to their activities, professional money launderers may work with corrupt individual(s) who specialise in the provision of otherwise legitimate services (e.g. bankers, lawyers, accountants) in addition to their criminal money laundering activity."

FATF said the report helps authorities understand how professional money launderers operate so that they can successfully target, prosecute and dismantle those who help make crime pay.

~ *Source: FATF*

Bank fined over AML failures

THE Hong Kong Monetary Authority (HKMA) has fined Shanghai Commercial Bank Limited HK$5m for anti-money-laundering failures.

The Authority said the bank had failed to establish and maintain effective procedures, and it has ordered the bank to submit a report prepared by an independent external advisor assessing whether the remedial measures implemented by it are sufficient to address the contraventions. Specifically, HKMA said the bank had not continuously monitored its business relationship with 33 customers by examining the background and purposes of their transactions that were identified as complex, and of unusually large amounts and of unusual patterns.

The bank had also failed to carry out customer due diligence measures in respect of certain pre-existing customers when transactions took place that were suspicious or unusual.

HKMA further said that Shanghai Commercial Bank also lacked effective policies and procedures for monitoring the handling of Management Information System (MIS) alerts including properly recording the follow-up actions taken and monitoring the review time, resulting in significant delay in alert clearance.

Solicitors Regulatory body sees rise in ML reports

REPORTS of money laundering involving firms in the UK have risen by two thirds since 2016, with 60 cases reported to the Solicitors Regulation Authority (SRA) in the first quarter of 2018, compared to just 36 in the final quarter of 2016.

In its annual Risk Outlook report, SRA said the legal market can be an attractive target for money launderers. Criminals want to instruct legal professionals to hold or transfer money because of the perceived legitimacy this offers.

Solicitors and firms are at an increased risk because they:

- regularly hold large sums of client money in pooled client accounts
- advise and transfer money in relation to property and financial transactions
- have access to financial markets.

SRA said one of the tools against money laundering is the suspicious activity reporting system, yet legal professionals submitted less than 1 percent of the total SARs to the National Crime Agency (NCA) in 2017.

SRA quotes NCA Director Donald Toon, who spoke at SRA's Compliance Officer Conference in 2017 as saying, "Solicitors are at the front line of the detection mechanism for money laundering but are worse than any other financial services sector in reporting suspicions. We get some very good quality reporting from the legal profession, but we get some that focuses very carefully on the identity, but not at all on the source of the funds – one half of the due diligence.

"Solicitors are a crucial source of information and intelligence on how criminals hide their assets. We have a very, very few who are criminally complicit, some who are careless and others who are unsure about their responsibilities."

In the report, SRA also shines the spotlight on conveyancing, which it says is particularly attractive to money launderers because of the large sums involved.

It said the UK Government's National Risk Assessment views conveyancing transactions as a serious risk, although it accepts that few solicitors are knowingly involved in illegal activity.

SRA said four in ten of the Suspicious Activity Reports (SARs) from the legal sector relate to conveyancing. In particular, residential conveyancing SARs have risen by 66 percent across the past two years. The faster turnover of house sales makes residential property a more common target for money launderers than commercial property. It is more usual for complex trusts to be involved in commercial conveyancing transactions.

SRA advises solicitors working in this field to take extra care, particularly when the transaction has the warning signs of potential money laundering, such as:

- purchases of very high value properties by overseas companies and trusts
- purchases involving money from high risk countries.

Paul Philip, SRA Chief Executive, said: "Our Risk Outlook helps solicitors to respond to the risks we see in the sector, supporting firms and protecting the public. Many of the risks we are highlighting are not new, but none of us can afford to be complacent.

"Although we know that very few solicitors would ever knowingly become involved in criminal or dishonest schemes, everyone needs to know the warning signs to look out for. It is important that law firms take steps to protect client money and information. Our recent warning notices on money laundering and dubious investment schemes aim to help them in this."

Organised crime can only operate if the criminals can move their money into the legitimate financial world. Solicitors who make money laundering possible, whether deliberately or unknowingly, can face serious consequences including criminal prosecution and regulatory sanctions.

For the first time, the SRA report is highlighting how claims are managed as a key risk. This follows concerns over issues such as firms failing to properly check on the validity of personal injury claims or charging fees which cannot be justified in areas such as payment protection insurance claims.

The Risk Outlook also reminds solicitors they must not draft the terms of non-disclosure agreements in a way that suggests a person may not report misconduct to a regulator or a law enforcement agency or make a protected disclosure.

Malaysia launches corruption clean-up measures

Malaysia's newly elected government, in power from May, came to power in part as to clear draft and corruption from the country. How well is it performing? Poorna Rodrigo *reports.*

THE Mahathir government has pledged a whole raft of measures to fight corruption. It includes setting up a new government anti-corruption wing and introducing new anti-bribery laws.

Given this government is the first in Malaysia's history that has not been dominated by the United Malays National Organisation, there is a general sense of optimism - but there is also growing pressure on the government now to walk the talk.

One such case currently under the spotlight is the scandal surrounding Malaysian sovereign wealth fund 1MDB (1 Malaysia Development Berhad) - set up under former Prime Minister Najib Razak - from which US$700 million is alleged to have been embezzled.

Gaining momentum

While investigations into the scandal started under the previous government, it has gained momentum under the new government, notably because Razak and his family have been accused of being part of the thefts. On July 3, Razak was arrested and charged for his alleged involvement in the scandal and Transparency International Malaysia (TI-M) was quick to hail the action.

"TI-M applauds the Malaysian Anti-Corruption Commission (MACC)'s swift and prompt action in arresting former Prime Minister Datuk Seri Najib Tun Razak who was believed to be involved in SRC International which was a subsidiary of 1MDB," it said in a statement.

TI claimed the arrest signified the completion of investigation by MACC, stressing that the resulting prosecution would be led by the newly-appointed Attorney General Tommy Thomas (in the post from June), who is a well-regarded litigator. The former Prime Minister has been charged on three counts of criminal breach of trust (CBT) under Section 409 of the Penal Code and one of abuse of power, according to TI-M.

Time and years

Speaking to *Commercial Crime International*, Transparency International Malaysia president Dr Dato' Akhbar Haji Satar however warned the proceedings "will take time and may take years" given "the complicated nature of the case and the difficulty in gathering evidence with documents and witnesses mostly overseas."

It will all depend on other countries' cooperation and effectiveness of law enforcement agencies, he said. Moreover, there may be overseas witnesses who may refuse to come and give evidence, he said. He added that Malaysia's whistleblower policies needed to be reviewed. Moreover, it may not be easy to recover the vast sums of money lost, he warned.

In a latest development, Malaysia's admiralty court granted an application by the government as well as 1MDB and two of its subsidiaries to sell a luxury superyacht 'Equanimity', trying to ward off further losses, Malaysia's national news agency *Bernama* said in a news report on August 24.

"Our next step is to get the vessel sold as it is a diminishing asset and the cost of maintenance is very high," Ong Chee Kwan, counsel for 1MDB and its subsidiaries 1MDB Energy Holdings Ltd and 1MDB Global Investment Ltd has been quoted as saying.

Unsurprisingly, Malaysia's ranking in Transparency International's Corruption Perception Index plunged to its worst ever slot last year, at 62nd place out of 180 countries. In 2016, the country was placed at 55th position, among 176 countries. Dr Satar says this is the "worst ranking since 1994" for Malaysia.

Nevertheless, there are efforts to rebuild integrity. "This being a new government, it is trying its best" to rid the country of corruption and fraud, said crime safety specialist from Malaysia-based Prevent Crime Now, Shamir Rajadurai.

Dr Mahathir Mohamad was sworn in as Malaysia's new Prime Minister on May 10, and within the same month he set up a special task force to look into 1MDB that was initially headed by former Attorney General Tan Sri Abdul Gani Patail.

On May 15, Dr Mahathir declassified an existing Auditor General's report on 1MDB in a further push for transparency. Mr Rajadurai said that the new Prime Minister has also asked all government department and ministries to identify weaknesses related to its relevant laws, procedures and policies, in a bid to clean up the government. "Obviously, the new government has a lot to prove," Mr Rajadurai said, adding it is making good progress.

Concrete action

In June, the Prime Minister agreed to the formation of a National Centre for Governance, Integrity and Anti-Corruption Centre (GIACC) responsible for planning, formulating strategies and evaluating policies in government to make sure it is corruption free. A Cabinet Special Committee on Anti-Corruption (JKKMAR) has also been created.

Continued on page 8/

Corruption/Bribery

Businessman charged over PDVSA bribery

A business executive who controlled multiple companies has been arrested in the US on foreign bribery charges for conspiring to make, and making, corrupt payments to an official of Venezuela's state-owned and state-controlled energy company, Petroleos de Venezuela S.A. (PDVSA), in exchange for favourable business treatment with PDVSA.

The 48-year-old US-Venezuelan citizen was arrested at Miami International Airport. He is charged with conspiring to violate the Foreign Corrupt Practices Act (FCPA) and paying bribes to a foreign official in violation of the FCPA.

According to the charge, the man and a co-conspirator paid at least $629,000 in bribes to a former PDVSA official in exchange for the official taking steps to direct PDVSA contracts to his companies; to give his companies priority over other vendors to receive payments, and to award his companies PDVSA contracts in US dollars instead of Venezuelan bolivars.

With his arrest, the US Justice Department has announced charges against 17 individuals, 12 of whom have pleaded guilty, as part of a larger, ongoing investigation by the US government into bribery at PDVSA.

from page 7 - Malaysia corruption

A special team led by the GIACC has been set up to submit a draft of the Political Funding Bill to the Cabinet that will impose criminal charges against civil servants who cause substantial financial losses to the government.

The bill would help anti-corruption officials investigate allegations that the government incurred losses due to negligence, non-compliance with requirements or procedures in government departments and agencies.

However, TI-M said in a statement that the proposed new law should be "widened to include more provisions covering politicians" and not just civil servants. "Very often the civil servants are actually pawns in a game being played by the bigger fish," it said adding: "In those cases such persons should also be brought to book especially if they are the mastermind in the whole corrupt transaction."

Taking stock

Marking his first 100 days in office on August 18, Dr Mahathir in a speech took stock of what his government has done to ensure good governance in Malaysia. He said his Pakatan Harapan (PH) government has fulfilled 21 of the 60 promises made in the election manifesto towards creating a corruption-free Malaysia.

Among these are that a new policy on the giving of gifts and donations to members of the civil service (from ministers to political secretaries) is being drafted.

And where the declaration of assets are concerned, the existing guidelines are being amended to expand the definition of 'members of the administration' so that even the Prime Minister and Deputy Prime Minister will also have to declare their assets.

Accordingly, an amendment will be made to the 'code of ethics for members of the administration and government members of Parliament, the Prime Minster said. From now on, such assets will be declared to the MACC so that there is openness and transparency, the Prime Minister said, insisting that he is trying to make Malaysia "known for integrity and not corruption".

What is needed more is "less theory" and more work showing "strong political will and leadership by example." ~ Transparency International Malaysia President Dr Dato' Akhbar Haji Satar

Less theory

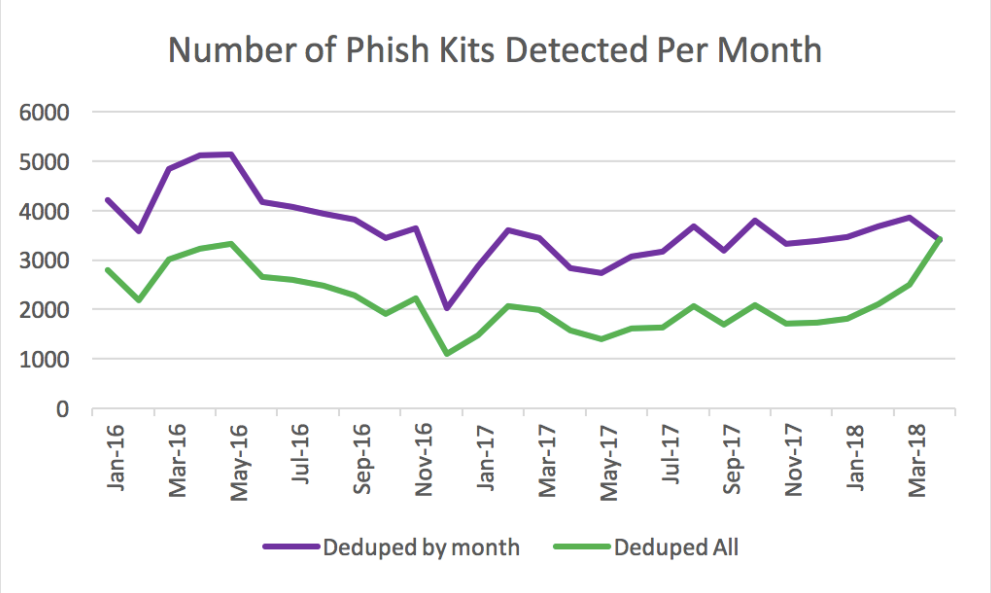
However, Dr Satar said what is needed more is "less theory" and more work showing "strong political will and leadership by example." For example, the GIACC and the Cabinet Special Committee are not "entirely new and instead have been rebranded by taking in a few existing departments," he said, adding that such efforts have failed to curb corruption in the past.

That said, Mr Rajadurai added the former governing party was being an effective opposition, looking for any weaknesses of the new government, effectively "keeping the necessary checks and balances" which is ultimately good for the general public.

Commoditisation of phishing kits fuel attacks

THE commoditisation of 'phishing kits' has made it much easier for cyber criminals to flourish through the easy creation of phishing sites, propelling phishing attacks in recent months.

According to research from MarkMonitor, the frequency of phishing attacks increased by 79 percent in the first quarter of 2018 compared to the same time last year.



Image/Source: MarkMonitor

"The primary reason for the proliferation of phishing is clear: when done right, it can be an incredibly effective way for cyber criminals to get hold of confidential customer data that can then be used for illicit activity," the company said.

Phishing kits consist of an archive folder (usually a .zip or .rar) that contains all of the code, information, graphics and other files necessary to create a phishing campaign with relative ease. These kits are then uploaded to a host — typically somewhere within the dark web, a private online marketplace or a message board.

While the kits themselves are created/authored by experienced online criminals with a deep knowledge of coding and phishing, once uploaded to a host they essentially allow anyone — even those with minimal technical prowess — to equip themselves with the necessary tools to launch sophisticated cyber attacks.

MarkMonitor said, "The proliferation of these kits means it should be no surprise to see the number of phishing attacks continuing to increase. The net is being cast even wider than before, with more victims falling prey to attacks created and set-up by a growing number of online criminals."

MarkMonitor has detected over 100,000 unique instances of phishing kits being used across the previous 28 months, equating to roughly 3,600 phishing kits detected per month (duplicates removed per month).

Interestingly enough, when de-duping (removing duplicate data) across the entire subset, the number of unique phishing kit detections drops to around 60,000 – indicating a fair number of phishing kit reuse.

Despite the efforts taken by criminals to prevent these kits being removed or shut down, MarkMonitor has developed innovative technology that can make a significant difference in mitigating the risks associated with them.

THE latest statistics from Action Fraud in the UK show that in June and July, victims reported losing £2m to cryptocurrency scams – an average of about £10,000 per person.

In the same period, 203 reports of this type of fraud were made to Action Fraud.

Action Fraud says fraudsters are cold calling victims and using social media platforms to advertise 'get rich quick' investments in mining and trading in cryptocurrencies.

Fraudsters will convince victims to sign up to cryptocurrency investment websites and to part with their personal details such as credit card details and driving licences to open a trading account.

The victim will then make an initial minimum deposit, after which the fraudster will call them to persuade them to invest again in order to achieve a greater profit.

In some cases, victims have realised that they have been defrauded, but only after the website has been deactivated and the suspects can no longer be contacted.

Cybercrime

Rise seen in extortion phishing

THE Financial Services Information Sharing and Analysis Center (FS-ISAC) in its August newsletter has warned that extortion phishing email campaigns are on the rise.

It said it has seen an up-tick in extortion phishing emails being shared.

One common campaign involves threat actors sending an email stating that they know the recipient's password, have installed malware on the computer, created videos of the recipient using adult websites through their webcam and have stolen the recipient's contacts.

The perpetrators are able to obtain leaked account credentials from data breaches and are using those leaked passwords when contacting victims.

FS-ISAC said its members have observed that the passwords used in the extortion emails may be from old LinkedIn accounts.

It is advising members that in addition to changing passwords, it is also important to verify the accuracy of the claim and determine if it is a hoax.

FS-ISAC has offered some pointers to guard against extortion phishing email campaigns;

- Confirm that malware was not placed on the system by running an antivirus scan.
- Ensure that the antivirus program uses updated signatures.
- Reimage the machine and reset passwords if malware is discovered.
- Speak with employees to determine any relevant information they may have.
- Provide social engineering training to employees and direct them to immediately report potential hoaxes.
- Implement spam filtering at the email gateway to filter out emails with known phishing indicators, such as known malicious subject lines.
- Implement Domain-Based Message Authentication, Reporting and Conformance (DMARC), a validation system that minimises spam emails by detecting email spoofing using Domain Name System (DNS) records and digital signatures.
- Adhere to best practices, such as those described in CIS, NIST and other similar frameworks.

To check if an email is a hoax:

- Determine if the email contains any specific knowledge about operations or if the language is generic and appears to be part of a mass mailing campaign.
- Conduct searches on keywords, the cryptocurrency wallet ID and sender's email address, as this may yield multiple examples of others affected by the same hoax.
- Check the cryptocurrency wallet ID for transactions to the wallet, which may provide insight into the threat actor's operations.
- Contact FS-ISAC and other information sharing resources to determine if other members report receiving similar emails.

FS-ISAC further said it has observed activity suggesting people are paying the ransom for some of these emails.

Tracking 42 bitcoin wallets cited in the extortion campaign, 30 victims had paid the blackmail demand – for a total of more than US$50,000 in a one-week period. One wallet alone received 2.54 bitcoins which equates to over US$18,000.

FS-ISAC cautions that there has been no suggestion that paying the ransom guarantees that the malicious emails will stop.

US man gets two years jail over $1m BEC scam

A US man was sentenced to two years in prison for his part in an international business email compromise scheme.

The 27-year-old and his co-conspirators stole over $1 million from victims while perpetrating their email scam.

From April 2015 through April 2016, victims received emails that appeared to be from trusted sources, including banking representatives and closing agents. In reality, the man's co-conspirators sent the emails, directing the victims to wire money to specific bank accounts, some of which were opened in the metro-Atlanta area.

In some instances, the co-conspirators hacked email accounts or they "spoofed" the email addresses, causing the email address to appear as if it were sent by a trusted source, when in reality, it was sent from a different account.

He recruited numerous individuals who agreed to allow him to use their bank accounts for the purpose of receiving large wires from unwitting victims. After receiving the wires, he directed his recruits on where to send the money, including to a number of financial institutions in Asia.

Together, they attempted to steal over $1 million during the timeframe of the conspiracy. He was sentenced to two years, three months in prison to be followed by three years of supervised release following his prison term.

He was also ordered to pay restitution in the amount of $176,059.03.

Singapore: financial firms told to tighten customer verification

THE Monetary Authority of Singapore (MAS) has issued a circular to all financial institutions, directing them to tighten their customer verification processes following a recent cyber attack at the country's largest healthcare group SingHealth in which personal information of 1.5 million individuals was illegally accessed and stolen in June.

MAS said with immediate effect, all financial institutions should not rely solely on a person's name, their National Registration Identity Card (NRIC) number, address, gender, race, and date of birth for customer verification.

Additional information must be used for verification before undertaking transactions for the customer.

Image: Pixabay

This may include, for instance, One-Time Password, PIN, biometrics, last transaction date or amount, MAS said.

MAS has also directed all financial institutions to conduct a risk assessment of the impact of the SingHealth incident on their existing control measures for financial services offered to customers, including transaction and inquiry functions.

"Financial institutions are to take immediate steps to mitigate any risks that might arise from the misuse of the compromised information. MAS will engage financial institutions on their risk assessments and mitigation steps," the Authority said.

For access to online financial services, banks in Singapore are already required to put in place two-factor authentication (e.g. PIN and One-Time-Password) at login to identify their customers.

Banks are also required to implement an additional layer of control to authorise high-risk transactions.

Financial institutions also have in place robust measures to verify customer identity. Personal information (name, NRIC number, address, date of birth, etc) is generally not used as the sole means of verification by financial institutions as these are often freely given out by members of the public for various purposes, such as when filling out lucky draw coupons or surveys.

Advanced techniques used in Thailand bank hacking cases

HACKERS used advanced hacking techniques to obtain data from more than 120,000 customers from two major banks in Thailand, *Xinhua.com* reports.

The hackers stole data from about 3,000 corporate customers who use an online bank guarantee service and 20,000 who had applied for credit online.

The attacks have been confirmed by the Bank of Thailand (BOT), who has vowed to step up security measures following the data breaches.

Executives of both banks said no suspicious transactions took place.

Payong Srivanich, President of Krung Thai Bank, one of the banks affected by the breaches said the bank was able to immediately stop the hacking after the bank's IT Division reported suspicious activities of stealing data.

The other bank affected by the security breach was Kasikornbank.

Its president Pipit Aneaknithi, said cybersecurity experts were able to quickly block the hackers from accessing the bank's internal data.

"The data that might have been leaked was public information of the customers including company's name and contact details," said Pipit, "there have been no reports of suspicious transactions from the hack."

He promised compensation to those affected.

Cybercrime

Clarksons reveals details of 2017 attack

UK shipping services company Clarkson PLC (Clarksons) has revealed details about the cyber attack which took place in November 2017.

The company said forensic investigation showed that an unauthorised third party had gained access to certain Clarksons' computer systems in the UK, from May 31, 2017 until November 4, 2017, copied data, and demanded a ransom for its safe return.

Clarksons said that the unauthorised access was gained via a single and isolated user account.

Upon discovering this access, Clarksons immediately disabled this account.

Through the investigation and legal measures, Clarksons were then able to successfully trace and recover the copy of the data that was illegally copied from its systems.

Clarksons said that while it was able to successfully trace and recover the copy of the data that was illegally copied from its systems, as a precautionary measure, the company has also been working diligently, in cooperation with law enforcement and forensic investigators, to determine what data may have been involved.

The company said it is notifying potentially affected individuals, adding that the potentially affected personal information varies by individual, but may include, among other details, information relating to insurance, passport, seafarers, bank accounts, payment card, financial, and address.

Clarksons said it had enhanced security measures to protect data and notified the necessary regulatory and law enforcement bodies across the relevant jurisdictions. However as a precautionary measure, Clarksons is also providing potentially affected individuals with information about the incident and about the further steps individuals may take to best protect their personal information.

It advises individuals to;

- Remain vigilant against incidents of identity theft and fraud by reviewing personal account statements for suspicious activity and to detect errors.
- Contact the account provider immediately if any suspicious activity is detected.

For potentially affected individuals residing in the US and for further details, go here.

~ Source: Clarksons

Shipbuilder gets cyber security compliance certification

DAEWOO Shipbuilding & Marine Engineering (DSME) has received approval in principle from Lloyd's Register (LR) for the DSME Smart Ship Solution, receiving the Cyber SECURE notation, which confirms compliance with LR's cyber security requirements for smart ships.

LR says the marine industry is far from immune to cyber attack incidents and security breaches, and the consequences can be far reaching.

The new level of connectedness presents the industry with both opportunities for improving safety, as well as introducing new areas of risk.

The hardware and software that control processes, systems and equipment can be vulnerable to attack, therefore numerous risks need to be identified, understood and mitigated to make sure that smart ship technologies are safely integrated into ship design.

"DSME has been focusing its efforts on developing an appropriate cyber security governance system, working closely with SEANET to mitigate the risk of introducing vulnerabilities to cyber-attack, " LR said.

COMMERCIAL CRIME International

Published monthly by Commercial Crime Services,
Cinnabar Wharf, 26 Wapping High Street, London E1W 1NG, UK
Tel: +44(0)20 7423 6960 Fax: +44(0)20 7423 6961
Email: ccs@icc-ccs.org Website: www.icc-ccs.org
Editor: Nathaniel Xavier Email: nathx73@yahoo.co.uk
ISSN 1012-2710