COMMERCIAL CRIME International
February 2018

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

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

Call for caution as piracy levels fall to 22-year-low

THE number of reported piracy attacks fell to a 22-year-low in 2017 but the ICC Commercial Crime Services' International Maritime Bureau (IMB) has cautioned that violence against crew is still high – particularly kidnapping, which saw the highest number of cases since 2006.

Last year, a total of 75 seafarers were kidnapped, 87 percent of these alone occurred in Nigerian waters (or 65 crewmembers). Previously, the highest number was in 2006 when the number of crew kidnapped was 77.

In 15 separate incidents, 91 crewmembers were taken hostage. Three crewmembers were killed in 2017 and six injured.

Overall in 2017, a total of 180 incidents of piracy and armed robbery against ships were reported to the IMB, according to its latest report.

It is the lowest annual number of incidents since 1995, when 188 reports were received.

Gulf of Guinea still risky

Last year, there were 36 reported incidents with no vessels hijacked in the Gulf of Guinea and 10 incidents of kidnapping involving 65 crewmembers in or around Nigerian waters. Globally 16 vessels reported being fired upon – including seven in the Gulf of Guinea.

Pottengal Mukundan, Director of IMB said, "Although the number of attacks is down this year in comparison with last year, the Gulf of Guinea and the waters around Nigeria remain a threat to seafarers.

"The Nigerian authorities have intervened in a number of incidents helping to prevent incidents from escalating," he said.

While the Nigerian authorities' efforts in assisting vessels attacked by pirates is to be commended, what is needed is a sustained long-term programme with a higher level of resources and deployment to ensure pirates are kept at bay.

Bulk carriers vulnerable

Bulk carriers remain vulnerable, 38 vessels were attacked by pirates during 2017, followed by product tankers (29), container ships (23), tankers (19), chemical tankers (13), general cargo vessels (12) and LPG tankers (11).

Somalia

Nine incidents were recorded off Somalia in 2017, up from two in 2016. In November, a container ship was attacked by armed pirates approximately 280 nautical miles east of Mogadishu.

The pirates, unable to board the vessel due to the ship's evasive manoeuvring fired two RPG rockets, both of which missed, before retreating.

Six Somali pirates were subsequently detained by European Union Naval Force, transferred to the Seychelles and charged with "committing an act of piracy" where they face up to 30 years' imprisonment, if convicted.

"This dramatic incident, alongside our 2017 figures, demonstrates that Somali pirates retain the capability and intent to launch attacks against merchant vessels hundreds of miles from their coastline," said Mukundan.

Southeast Asia

Indonesia recorded 43 incidents in 2017, down from 49 in 2016. The IMB report notes that Indonesian Marine Police patrols continue to be effective in the country's 10 designated safe anchorages.

Continued on page 2/

In This Issue of CCI

PIRACY
Call for increased efforts 2
IMB PRC goes from strength to strength 3
FRAUD
Australia investment fraud increases 5
EU Public Prosecutor and VAT fraud 6
MONEY LAUNDERING
UK world-first register to tackle ML 8
Banks fined over compliance failures 9
CYBERCRIME
Chief information officers identify main threats for 2018 10
South Korea: new bank guidelines for cryptocurrency trading 11

Cargo shipowners call for increased efforts

THE International Association of Dry Cargo Shipowners (INTERCARGO) has expressed deep concern over piracy and crew kidnaping in the Gulf of Guinea, and has called for a doubling-up of efforts to tackle the problem.

The association referred to a piracy incident off Nigeria in mid-December, where it was reported that a 57,000 dwt bulk carrier, en route from Lagos to Port Harcourt, was attacked by pirates 35 miles south of Brass, Nigeria.

Before the ship was released, the pirates kidnapped 10 crewmembers, including officers, and fled.

INTERCARGO said the incident is a vivid reminder that piracy as an organised criminal activity remains a significant threat to international shipping, trade, and the people who serve it.

"It must be ensured that there is no relaxation or step back in the measures in place against piracy; moreover, efforts and necessary resources fighting piracy must be upgraded primarily in the most vulnerable regions, such as West Africa, the Gulf of Aden, and South East Asian sea corridors.

"INTERCARGO has been participating throughout 2017 in numerous industry meetings and initiatives with all the involved stakeholders to ensure that industry guidelines remain relevant and that optimal countermeasures are duly allocated in the coming years, in sea and on land as required, to eradicate the plague of modern piracy."

from page 1 - global piracy attacks fall

In the Philippines, however, the number of reported incidents has more than doubled, from 10 in 2016 to 22 in 2017.

The majority of these incidents were low-level attacks on anchored vessels, mainly at the ports of Manila and Batangas. Vessels underway off the Southern Philippines were boarded and crew kidnapped in the first quarter of 2017.

However, alerts broadcast by the IMB's Piracy Reporting Centre (PRC), on behalf of the Philippine authorities, have since helped to avoid further successful attacks.

Underreporting still a problem

IMB is reminding members to report incidents to its Piracy Reporting Centre (PRC). The level of underreporting in the Gulf of Guinea is still considerably high – at 62 percent. In these waters for the January to December 2017 period, the total number of piracy attacks reported to IMB was 36 while the number of incidents recorded by the Community of Reporting was 95.

On a related issue Mr Mukundan said, "Leveraging on the experience of the past decade it would make sense to consider developing a simplified worldwide system to which vessels can easily report attacks and through which the IMB Piracy Reporting Centre and the regional reporting centres share information freely on attacks and threats to vessels."

Launched in 1991, the IMB PRC is a 24-hour manned centre that provides the maritime industry, governments and response agencies with timely and transparent data on armed robbery incidents received directly from the master or owner of vessels wherever they are in the world. The IMB PRC's prompt forwarding of reports and liaison with response agencies, its broadcasts to shipping via Inmarsat Safety Net Services and email alerts to chief security officers, all provided free of cost, has helped the response against piracy and armed robbery and the security of seafarers, globally.

Piracy Reporting Centre grows from strength to strength

LOCATED in an office tower block in the heart of Malaysia's capital city Kuala Lumpur is the location for one of ICC Commercial Crime Services (CCS)' important services.

Set up in 1992 in response to the outrage within the shipping industry at the alarming growth in piracy, the International Maritime Bureau(IMB) 's Piracy Reporting Centre (PRC) continues to provide unique value to the shipping industry and has grown from strength to strength.

Starting with just three staff members, the organisation's Kuala Lumpur office now employs 41 people – 15 of whom work solely on all things piracy-related. The others were taken on to fill roles after the Kuala Lumpur's office portfolio expanded to include what its London counterpart does – analysts dedicated to tackling commercial crime.

"We have seen a rise in the numbers of ships and shipping companies contacting us, asking for advice. More shipping companies/Masters are also requesting us to participate in their drills where they recreate scenarios of pirate attacks. These drills enable the ship's crew to respond to the emergencies more effectively with PRC's assistance, as would happen in a real-life event," says Noel Choong, IMB PRC regional manager.

Choong who has worked with the organisation since 1997, has been the driving force of the PRC, ensuring that it remains relevant and continues to grow its presence and services worldwide. One such vital service is the IMB's quarterly and annual piracy report.

"We are the only agency that produces and publishes reports of such attacks on a global scale which contain transparent statistics, providing analysis of attacks and piracy trends," says Choong.

The PRC, which operates 24 hours every day, is equipped with 10 screens which can trace and monitor ships at sea. In addition, the systems also allow it to view weather data and communicate with response agencies.

"A key strength of PRC is being able to link up with the authorities of different countries, to share our information with them so that they are able to respond immediately, as soon as we receive reports," says Choong.

The PRC has to date assisted many ships in distress and has saved many lives and property at sea. The PRC also transmits regular SITREPs and Warnings by satellite broadcast to ships at sea via Inmarsat C EGC Safety Net so that ship Masters can be alerted and take necessary actions to avoid being attacked.

Piracy reports are also posted on the IMB's website at www.icc-ccs.org/index.php/piracy-reporting-centre/live-piracy-report - by posting the information on the internet, ship owners and authorities ashore as well as ships at sea can access these updates regularly and make informed decisions and assess associated risks with high-risk sea areas.

Choong is also particularly proud of a PRC initiative that began five years ago – the Maritime Security Hotline, which allows seafarers, port workers, shipping agents and other concerned parties to report information they may have seen, heard or known of relating to any security threats.

Continued on page 4/

from page 3 - IMB Piracy Reporting Centre

These calls are treated in strict confidence and will be passed on to the relevant authorities for their action. The list of authorities getting involved is growing and we are continuously expanding cooperation and looking for more organisations to join this initiative," he says.

Choong adds, "People may come across certain information that they want to report but not necessarily to the authorities or to their employers, so we offer them a neutral, independent avenue to do so.

Sometimes the information is crucial for certain incident investigations that may save lives and prevent crime".

Choong adds that it is vital that shipmasters and owners report all actual, attempted and suspected piracy and armed robbery incidents to the IMB PRC. Only with official reports can the PRC inform the concerned governments which leads to them increasing resources to tackle this problem.

This is important for the safety of seafarers and ships at sea and benefits the shipping industry.

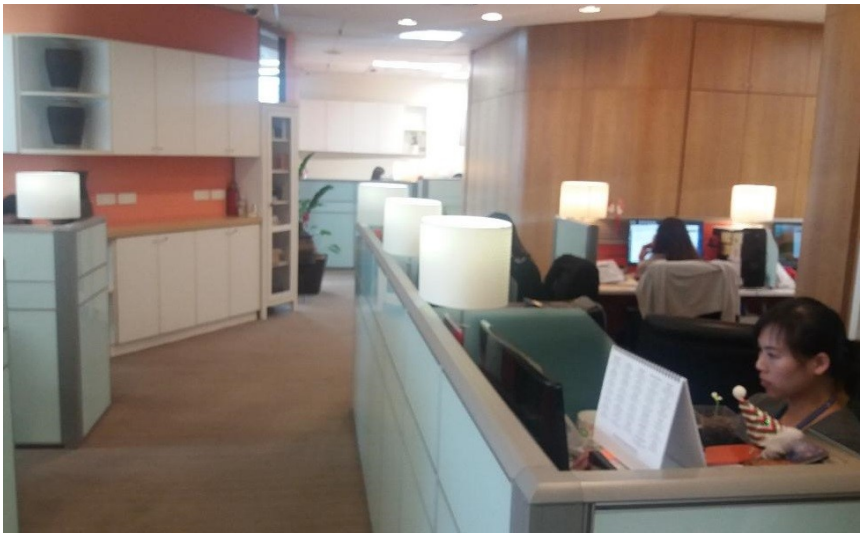
"This first step in the response chain is vital to ensuring that adequate resources are allocated by authorities to tackle piracy. Transparent statistics from an independent, non-political, international organisation can act as a catalyst to achieve this goal."

* IMB's website offers helpful tips and advice to masters of ships, including piracy hotspots and taking precautionary measures. For details go to https://www.icc-ccs.org/index.php/piracy-reporting-centre

How to contact the IMB PRC

ICC IMB (Asia Regional Office),
PO Box 12559,
Kuala Lumpur,
50782,
Malaysia.
Tel: + 60 3 2078 5763
Fax: + 60 3 2078 5769
E-mail: imbkl@icc-ccs.org / piracy@icc-ccs.org

24 Hours Anti-Piracy HELPLINE
Tel: + 60 3 2031 0014



IMB PRC – Key services

- Issuing daily status reports on piracy and armed robbery to ships via broadcasts on the Inmarsat-C SafetyNET service.
- Reporting piracy and armed robbery at sea incidents to law enforcement and the International Maritime Organization.
- Helping local law enforcement apprehend pirates and assist in bringing them to justice.
- Assisting shipowners whose vessels have been attacked or hijacked.
- Assisting crewmembers whose vessels have been attacked.
- Providing updates on pirate activity via the internet.
- Publishing comprehensive quarterly and annual reports detailing piracy statistics.
- The services of the PRC are provided free of charge to all ships irrespective of their ownership of flag.

Australia sees rise in investment fraud numbers

AUSTRALIANS reported losses of more than $31.15 million due to investment scams in 2017, according to the latest data from the Australian Competition and Consumer Commission (ACCC).

This represented a staggering 32 percent increase compared to 2016, where investment scam losses totalled $23.63 million, according to figures published by Scamwatch, a division of ACCC.

In December alone, reported losses involving investment schemes was $2.9 million.

Australians reported a total of 161,572 scams in 2017, amounting to more than $89.4m in losses.

The main types of scam in terms of amounts lost were investment; dating and romance; other business, employment and investment; and upfront payment and advanced free scams.

Phishing was the top scam reported to ACCC (26,121 reports), followed by identity theft and false billing.

Most of the scams were committed over the phone, followed by email and social networks.

Top 5 scams (Amounts Loss)

Investment	$31.15 million
Dating & Romance	$20.3 million
Business, employment & investment	$5.26 million
Upfront payment & advanced fee	$4 million
Other buying & selling	$3.5 million

Top 5 scams types reported

Phishing	26,121
Identity Theft	15,697
False Billing	13,435
Unexpected Prize & Lottery	12,703
Other buying & selling	10,279

Scam delivery method

Retirement fund investors targeted

SYNDICATES in Malaysia are using fake agreements to dupe retirement fund contributors into withdrawing their savings and investing in high-yield schemes.

Local press reports quoted an Islamic finance consultant as saying that syndicates were getting smarter, and had introduced a new technique of using bogus agreements to convince contributors to invest or make withdrawals.

Previously, the syndicates used to meet people they contact at random and coax them with various promises and sweet talk, the consultant said.

To win the confidence of those who wish to invest in their schemes, they offer gifts to demonstrate that they will definitely be able to get the promised returns.

"Now, they are using a new technique. Besides the gifts, the latest technique is to use contract documents. If there is a contract, the public may think it's 'okay' (legitimate). However, when it is brought to the bank or the Employees Provident Fund, the document is found to be false and poses problems for the contributors," he told news agency *Bernama.*

The consultant added that contributors approached by such groups should carry out their own checks on the companies before deciding whether or not to invest.

European Public Prosecutor set to tackle VAT fraud

Companies and citizens defrauding European Union (EU) revenue collection (including customs duties and cross-border VAT fraud) and spending programmes, may from 2020 face direct criminal proceedings brought by a European Public Prosecutor (EPPO). Keith Nuthall and Diana Yordanova *report from Brussels*

IT has been a long time coming. The idea of creating a European Public Prosecutor, able to investigate and prosecute cases independently of national judicial authorities, was mooted as long ago as 2000 by an EU expert group in a report called 'Corpus Juris'.

Since then, it has been a slow crawl to the launch of this potentially powerful institution. The right to create an EPPO was written into the EU's Lisbon treaty in 2009, but it was only this past October (2017) when the EU Council of Ministers approved establishing this new institution.

Using the EU's enhanced cooperation procedure for passing laws that do not cover the entire EU, the EPPO will operate in 20 of the current 28 EU member states - Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Estonia, Germany, Greece, Spain, Finland, France, Italy, Latvia, Lithuania, Luxembourg, Portugal, Romania, Slovenia and Slovakia.

Protecting taxpayers' money

The new EPPO will have more power than the current EU anti-fraud unit OLAF, which has to persuade national prosecutors to act after it builds up a case. But with eight member states (seven once Britain quits the EU) remaining outside the EPPO's jurisdiction, OLAF will remain in business detecting fraud in these countries. Detailed cooperation systems between it and the EPPO have yet to be agreed.

The prosecutor will operate out of Luxembourg and will start chasing and launching cases in three years' time, if the office's establishment goes according to plan. He or she will work with 20 European Prosecutors (one per participating country), two of whom will be deputies to the chief, an administrative director and dedicated technical and investigative staff. They will work with European Delegated Prosecutors located in participating member states and who will generally carry out investigations and prosecutions in their own countries, working with national police and applying national laws.

Welcoming the decision, Urmas Reinsalu, the justice minister for Estonia (which held the EU presidency until this past December), Minister of Justice, said his office would "help to protect our taxpayers' money." He added: "Even when criminals act across borders, we can now make sure they are brought to justice and that taxpayers' money is recovered."

Image: Activedia/Pixabay

VAT fraud

Given the EU uses VAT and import duties to help fund its activities, frauds against these taxes, including smuggling and missing trader cross-border VAT scams will fall within the jurisdiction of the new prosecutor. So, will public procurement scams, bribery, corruption and embezzlement regarding the EU's multifarious spending programmes, which span agriculture, industrial support, research, regional development, energy infrastructure and more.

With the EU's budget being €157 billion in 2017, and the estimated cost of fraudsters targeting the EU budget or setting up complex VAT fraud, being at least €50 billion of potential revenue annually, the scope for prosecution is wide.

Of course, businesses will not want to be involved in a European prosecution, either as a participant (maybe unwittingly so) or as a victim, and the goal of establishing this office is that such crimes are more likely to be pursued than they are now.

At present, national law enforcers only are responsible for prosecuting such crimes, and with the EU footing the bill of spending programmes, there is less incentive for these prosecutors to act than target scams involving nationally-funded government policies. A note from the EU executive the European Commission, said: "National law enforcement efforts are fragmented across member states, which do not always take the action required to tackle crimes against the EU budget.

Today, only around 50 percent of the judicial recommendations transferred by OLAF to the national prosecution authorities lead to an indictment. The indictment rates vary considerably among member states."

So, the EPPO could be good news for companies wanting less smuggling that can undercut legitimate trades and for those wanting to fairly bid for government

Continued on page 7/

from page 6 - European Public Prosecutor to be established

contracts. For those who have weak monitoring of potentially corrupt staff, however, the EPPO could be a problem.

A welcome move

But "with fraud costing organisations an estimated 5 percent of revenue annually, the ACFE [Association of Certified Fraud Examiners] is always encouraged to see official bodies acknowledging that it is a serious issue that needs to be addressed", Bruce Dorris, ACFE vice president and programme director told *Commercial Crime International.*

Dorris added that cross-border fraud investigations can often prove difficult and time consuming, so creating a multinational, cooperative organisation that investigates and prosecutes fraud, demonstrates the EU's commitment to stamp out the problem.

Another anti-crime organisation, React - The Anti-Counterfeiting Network, also welcomed the move. It says 90,000 cases it tackles annually are cross-border: "For example, goods are coming from Turkey, then they are imported in Germany and disassembled in several other countries… I find the EPPO adequate, efficient, logical and very important for us", said React's managing director, Ronald Brohm. Under the current system, it sometimes "takes ages" for EU law enforcement authorities to tackle cross-border cases. "The new EPPO will have prosecution power and this is what will make it different and efficient. It is a major step ahead and I am in favour", Brohm emphasised.

The UK-based Anti-Counterfeiting Group (ACG) expected more rapid communication, speedier exchanges of information and greater collaboration because of the EPPO.

"Depending on the outcome of Brexit negotiations, we also believe that a central structure would encourage and enable ACG members to engage more easily with EU, cross border enforcement authorities," said ACG communications and events manager, Carol Levin.

She however warned that differences between criminal laws across the EU could impede the EPPO's effectiveness.

Close cooperation

As for liaison with OLAF, which will continue to operate after the EPPO's establishment, European Commission's spokesman Christian Wigand said the eight member states opting out from the EPPO will still be able to liaise with the prosecutor.

There are two possibilities - to post liaison officers to the EPPO or designate specific contact points. As for the other 20 countries, OLAF will need "to establish and maintain a close cooperation aimed at ensuring the complementarity of their mandates, and avoiding duplication", Wigand told *Commercial Crime International.* "OLAF will not open any administrative investigations parallel to an investigation conducted by the EPPO. Conversely, in cases where the EPPO is not conducting an investigation, OLAF will retain its power to start an administrative investigation on its own initiative," he noted.

EU bodies and national authorities would need to report to EPPO any suspected criminal offences falling within its expertise. OLAF on its side will have to report a case to EPPO if it falls within the new body's competence. Companies and individuals will also be able to report cases to the EPPO as well as national criminal investigative bodies.

Fraudsters made £1.4m from bogus healthcare investment scam

FOUR men in the UK who tricked vulnerable retirees into investing in a healthcare share scheme made a profit of £1.4 million.

The group set up a company Symbiosis Healthcare Plc (Symbiosis), purporting to offer "healthcare solutions" and organised the selling of Symbiosis shares.

They published misleading statements and exaggerated promotional material which was designed to fool investors.

Additionally, investors were cold-called by brokers, and mis-sold shares in Symbiosis.

Despite promises to investors of large profits, and extravagant claims about the operation and expansion of a network of medical clinics in Dubai and elsewhere, in reality the shares in the company were effectively worthless. In total, over 300 investors lost just over £1.4 million through the scheme.

The four have now received sentences between nine months and 8 years in prison following a prosecution brought by The Financial Conduct Authority in court.

Commenting on the case, Mark Steward, Director of Enforcement and Market Oversight at the FCA, said, "The perpetrators of this scheme repeatedly misled investors for their own gain. The FCA is committed to ensuring that the operators of unauthorised investment schemes are brought to justice and are accountable for their misconduct."

UK: New property register to crackdown on ML

A world-first register revealing owners of overseas companies buying property in the UK will go live by early 2021 to crack down on criminal gangs laundering dirty money in the UK, the UK government has announced.

More than £180 million worth of property in the UK has been brought under criminal investigation as the suspected proceeds of corruption since 2004.

Over 75 percent of properties currently under investigation use offshore corporate secrecy - a tactic regularly seen by investigators pursuing high-level money laundering.

The Department for Business, Energy and Industrial Strategy's register will require overseas companies that own or buy property in the UK to provide details of their ultimate owners.

This will help to reduce opportunities for criminals to use shell companies to buy properties in London and elsewhere to launder their illicit

Image: Pixabay/Geralt

proceeds by making it easier for law enforcement agencies to track criminal funds and take action.

Last month in the House of Lords the government committed to publishing a draft bill this summer and introducing it in Parliament by next summer. Following legislation, the register would go live by early 2021.

UK Business Secretary Greg Clark said, "We are committed to protecting the integrity and reputation of our property market to ensure the UK is seen as an attractive business environment – a key part of our Industrial Strategy.

"This world-first register will build on our reputation for corporate transparency as well as helping to create a hostile environment for economic crimes like money laundering. The register will also provide the government with greater transparency on overseas companies seeking public contracts."

US seeks closer info sharing with financial institutions

THE US Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) has launched the FinCEN Exchange programme to enhance information sharing with financial institutions.

As part of this program, FinCEN, in close coordination with law enforcement, will convene regular briefings with financial institutions to exchange information on priority illicit finance threats, including targeted information and broader typologies.

This will enable financial institutions to better identify risks and focus on high priority issues and will help FinCEN and law enforcement receive critical information in support of their efforts to disrupt money laundering and other financial crimes. FinCEN said private sector participation in the programme is strictly voluntary, and it does not introduce any new regulatory requirements. It also does not replace or otherwise affect existing mechanisms by which law enforcement engages directly with the financial industry.

Since 2015, FinCEN has convened over a dozen special briefings in five cities with over 40 financial institutions and multiple law enforcement agencies. In connection with these briefings, FinCEN, working closely with law enforcement, issues requests pursuant to Section 314(a) of the USA PATRIOT Act related to investigations and provides associated financial typologies. The briefings also have proved useful to financial institutions, helping them focus on specific priorities and better identify risks.

FinCEN Exchange will build on the success of these efforts by convening more regularly scheduled and as needed operational briefings across the nation with law enforcement, FinCEN, and financial institutions to exchange information on priority illicit finance and national security threats.

In consultation with law enforcement, FinCEN will invite financial institutions to participate based on a variety of factors, including whether they may possess information relevant to a particular topic.

The information shared, whether through Section 314(a) of the USA PATRIOT Act or other authorities, will often include information intended to support specific lines of investigation or broader typologies related to a particular illicit finance threat. After receiving information at a FinCEN Exchange operational briefing, financial institutions will be better equipped to incorporate responsive information into suspicious activity reports.

Britain enhances anti-ML systems

UNITED Kingdom is taking action to further enhance its anti-money laundering systems and ensure that professionals work with the financial sector to uphold higher standards.

The steps are part of a recently-announced cross-government anti-corruption strategy which provides a framework to guide UK government action to tackle corruption for the period to 2022.

Among the measures include;

- The creation of a new Office for Professional Body Anti-Money Laundering Supervision (OPBAS), hosted by the Financial Conduct Authority (FCA), to help and ensure that professional body AML supervisors implement their supervisory obligations to a consistently high standard, and work across the regime to share best practice and facilitate the flow of information with law enforcement.
- Increasing the analytical capability of the Joint Money Laundering Intelligence Taskforce, and continuing to expand its membership to include more banks and other financial services firms.
- The UK's National Crime Agency (NCA) estimates up to £90 billion of illicit funds are laundered through the UK each year.

Other measures include;

- Strengthening the ability of UK authorities to investigate and prosecute grand corruption and return assets, working with international partners.
- Further enhancing anti-money laundering and counterterrorist financing capability.
- Enacting the Criminal Finances Act in April 2017. This strengthens the UK's ability to tackle money laundering, corruption, tax evasion and terrorist financing.
- Enhancing anti-money laundering (AML) and counter-terrorist financing capability. Ensuring that the UK's regulations conform to the latest international standards, while reforms to the AML supervisory regime will ensure there is effective supervision of businesses that could facilitate money laundering.

Further to these steps, the UK government also announced the setting up of a National Economic Crime Centre within the NCA - a multi-agency centre which will plan, task and coordinate operational responses across different agencies bringing together the UK's capabilities to tackle economic crime more effectively.

Banks fined over compliance failures

TAIWAN's Mega Bank in the US has been fined $29 million for not complying with anti-money laundering (AML) laws by the US Federal Reserve Board.

The Federal Board said recent checks on the Bank's branches in New York, Chicago and San Francisco disclosed significant deficiencies relating to risk management and compliance with applicable federal and state laws, rules, and regulations relating to AML compliance, including the Bank Secrecy Act.

The statement said that the Federal Board needed the company to improve its oversight and control in terms of money laundering prevention. The statement said the Bank must exercise necessary steps to make sure the laws are not overlooked.

All three branches have been notified of the details regarding the fine and have been told that the inspection of the branches revealed "significant deficiencies" in its operations, risk management and compliance controls in relation to anti-money laundering and bank secrecy laws. In 2016, the US Department of Financial Services fined Mega Bank $180 million for violating New York's anti-money laundering laws. DFS's examination had uncovered that Mega Bank's compliance programme was a 'hollow shell', and DFS's examination found that the Bank's head office was indifferent toward risks associated with transactions involving Panama, recognised as a high-risk jurisdiction for money-laundering.

Separately, The Office of the Comptroller of the Currency (OCC) in US recently issued a $70 million fine against Citibank for failing to comply with the OCC's 2012 consent order related to Bank Secrecy Act (BSA) and AML deficiencies.

In its 2012 order, the OCC cited the bank for BSA violations, deficiencies in its compliance programme, failing to file suspicious activity reports, and weaknesses in controls related to correspondent banking.
The agency found that the Bank has not achieved compliance with the OCC's 2012 order.

The Bank paid the assessed penalty to the US Treasury.

Chief information officers identify main threats in 2018

WHAT are the main threats related to cyber risk and info security are chief information security officers (CISOs) worried about for 2018?

A survey of 612 CISOs and information security (infosec) professionals by risk and compliance firm Opus in partnership with Ponemon Institute could offer some insight.

After the year that was 2017, most CISOs believe that cyber threats are getting worse, and that their jobs are becoming much harder.

67 percent believe their companies are more likely to fall victim to a cyberattack or data breach in 2018.

- Cyber risk and data breaches are a key concern for CISOs as we enter 2018. High-profile data breaches regularly made headlines in the past year and show no signs of slowing down, with 67 percent concerned they'll fall victim to a data breach or attack this year. And, 60 percent of CISOs reported their concerns about data breaches from third parties has increased.

- The top factors driving their concerns are their organisation's inability to protect sensitive and confidential data from unauthorised access; inability to keep up with the stealth of the attackers; and failure to control third parties' use of sensitive data.

CISOs find the human factor is the greatest security threat.

- CISOs are more worried about people making mistakes that lead to a cyberattack than about technology. 70 percent of CISOs said "lack of competent in-house staff" was the threat they worried most about for 2018 — topping the list over even a data breach or cyberattack.

- Besides staffing concerns, an organisation's employees are also a major source of cyber risk. 65 percent of CISOs predict a careless employee will fall victim to a phishing scam that will result in credential theft. Though this is a top concern, 54 percent of CISOs fear they will not be able to reduce employee negligence.

Securing disruptive technologies will be a major challenge.

- The technology landscape is constantly evolving, and CISOs have to keep up with the latest trends as organisations embrace more digital offerings. In the area of disruptive technologies, CISOs consider IoT devices the most challenging to secure, followed by mobile devices and the cloud.

Managing an already stressful role with less resources and more cyber risk.

- CISOs face the daily pressure of keeping company and customer information secure while also supporting business growth. Not surprisingly, the stress is taking a toll. 69 percent of CISOs anticipate their roles will be even more stressful in 2018. This is due in part to increasing cyber threats, information security budgets that will decline or remain flat, and the significant costs in the event of a data breach.

- 45 percent fear they will lose their job, and 56 percent believe they will be unable to recover sensitive and confidential data after a breach. These concerns are even pushing CISOs out of IT security positions completely.

It is not all bad news, however. Despite the clear and imminent cyber risks, some CISOs see a path forward for improving their cybersecurity posture - 37 percent of respondents, in fact. The top pathways to stronger cybersecurity include cyber intelligence improvements, improvement in staffing, reduction in complexity and improvement in technologies.

Though 2017 was a dismal year for the infosec community, perhaps lessons learned will help spur organisations to better risk management.

CISOs and Third-Party Risk

One recurring concern CISOs cited in the study was the risk associated with doing business with third party vendors and suppliers. 42 percent of CISOs worry about experiencing a third-party data breach, and 44 percent worry that a third party will misuse or share confidential information with other third parties.

Their concerns are legitimate. Third-party data breaches are up 7 percent over last year, with major, globally-recognised companies falling victim. Fortunately, there are ways to reduce risk by following third party risk management best practices. CISOs are recognising this reality.

Forty-two percent believe better visibility into the sensitive data accessed and used by third parties, vendors, business partners and contractors would improve an organisation's cybersecurity.

The full report can be downloaded at https://www.opus.com/resource/2018-ciso-survey-ponemon-institute/

Two US states issues cryptocurrency warning

A lot is being said about Bitcoin in the news of late and against this backdrop the Idaho Finance Department in US has cautioned about investments involving cryptocurrency.

"Investors should go beyond the headlines and hype to understand the risks associated with investments in cryptocurrencies, as well as cryptocurrency futures contracts and other financial products where these virtual currencies are linked in some way to the underlying investment," said Gavin Gee, director Of the Department of Finance.

His department drives home the message that current common cryptocurrencies include Bitcoin, Ethereum and Litecoin are not insured or controlled by a central bank or other governmental authority, and therefore cannot always be exchanged for other commodities, and are subject to little or no regulation.

A survey of state and provincial securities regulators by the North American Securities Administrators Association (NASAA), of which the Idaho Department of Finance is a member, reports that 94 percent believe there is a "high risk of fraud" involving cryptocurrencies.

Regulators also were unanimous in their view that more regulation is needed for cryptocurrency to provide greater investor protection. "The recent wild price fluctuations and speculation in cryptocurrency-related investments can easily tempt unsuspecting investors to rush into an investment they may not fully understand," Gee said.

Recently, NASAA identified Initial Coin Offerings (ICOs) and cryptocurrency-related investment products as emerging investor threats for 2018. Unlike an Initial Public Offering (IPO) when a company sells stocks in order to raise capital, an ICO sells "tokens" in order to fund a project, usually related to the blockchain.

The token likely has no value at the time of purchase. Some tokens constitute, or may be exchangeable for, a new cryptocurrency to be launched by the project, while others entitle investors to a discount, or early rights to a product or service proposed to be offered by the project.

Separately in the Alaska state securities regulator has also issued a warning about the risks associated with cryptocurrency investments, saying they are potentially susceptible to cybersecurity breaches or hacks.

South Korea: new bank guidelines for cryptocurrency trading

BANKS in South Korea will now only allow cryptocurrency trading through real-name bank accounts linked to cryptocurrency exchanges.

Under the new guideline which took effect from the end of last month, users who want to make cryptocurrency transactions must have a bank account under their real name at the same bank with cryptocurrency exchanges.

Those who do not have their real-name account at the same bank will only be allowed to withdraw money from their existing bank account.

To make new deposits, they are required to open a new bank account under their real name at the same bank with the exchanges.

The rule introduced by the Financial Services Commission, is aimed at ensuring banks identify their customers and comply with their anti-money laundering (AML) obligations in cryptocurrency transactions.

Minors under the age of 18 and foreigners will not be allowed to open new bank accounts linked to cryptocurrency exchanges to deposit their money for cryptocurrency trading. Existing anonymous bank accounts that have been used to trade cryptocurrencies will no longer be in use.

In early January the Korea Financial Intelligence Unit (KoFIU) and the Financial Supervisory Service conducted joint inspections on six commercial banks that offer bank accounts to cryptocurrency exchanges and found a number of loopholes in banks' compliance with AML obligations.

Based on the results of our inspections, KoFIU came up with a 'Cryptocurrency-related AML Guideline' to address such loopholes and clarify obligations and responsibilities of financial institutions to prevent cryptocurrency related money laundering.

The FSC expects the measures announced today to reduce room for cryptocurrency transactions to be exploited for illegal activities such as crimes, money laundering and tax evasion. Under the guideline, banks are allowed to refuse to offer bank accounts if cryptocurrency exchanges do not provide information upon their request.

The guideline will also caution banks against offering accounts to cryptocurrency exchanges without careful consideration.

Gang used 'ransomware-as-a-service' to carry out attacks

AUTHORITIES in Romania have arrested three individuals who are suspected of infecting computer systems by spreading the CTB-Locker (Curve-Tor-Bitcoin Locker) malware - a form of file-encrypting ransomware.

Two other suspects from the same criminal group were arrested in Bucharest in a parallel ransomware investigation linked to the US.

The case illustrates the "Ransomware-as-a-service" model, as the suspects acquired the malware through specific developers on the Darknet.

Six houses were searched in Romania as a result of a joint investigation carried out by the Romanian Police (Service for Combating Cybercrime), the Romanian and Dutch public prosecutor's office, the Dutch National Police, the UK's National Crime Agency, the US FBI with the support of Europol's European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT).

Investigators seized a significant amount of hard drives, laptops, external storage devices, cryptocurrency mining devices and numerous documents. The criminal group is being prosecuted for unauthorised computer access, serious hindering of a computer system, misuse of devices with the intent of committing cybercrimes and blackmail.

In early 2017, the Romanian authorities received detailed information from the Dutch High Tech Crime Unit and other authorities that a group of Romanian nationals were involved in sending spam messages.

This spam was specifically drafted to look like it was sent from well-known companies in countries like Italy, the Netherlands and the UK.

The intention of the spam messages was to infect computer systems and encrypt their data with the CTB-Locker ransomware aka Critroni. Each email had an attachment, often in the form of an archived invoice, which contained a malicious file. Once this attachment was opened on a Windows system, the malware encrypted files on the infected device.

CTB-Locker was first detected in 2014 and was one of the first ransomware variants to use Tor to hide its command and control infrastructure. It targets almost all versions of Windows, including XP, Vista, 7 and 8. Once infected, all documents, photos, music, videos, etc. on the device are encrypted asymmetrically, which makes it very difficult to decrypt the files without the private key in possession of the criminals, which might be released when victims pay the ransom.

In addition to the spread of CTB-Locker, two people within the same Romanian criminal group are also suspected of distributing the Cerber ransomware. They were suspected of contaminating a large number of computer systems in the United States. The US Secret Service has subsequently started an investigation into the Cerber ransomware infections.

This case illustrates the Crime-as-a-Service (CaaS) model, as the services were offered to any criminal online. The investigation in this case revealed that the suspects did not develop the malware themselves, but acquired it from specific developers before launching various infection campaigns of their own, having to pay in return around 30 percent of the profit.

This modus operandi is called an affiliation program and is "Ransomware-as-a-service", representing a form of cybercrime used by criminals mainly on the Dark Web, where criminal tools and services like ransomware are made available by criminals to people with little knowledge of cyber matters, circumventing the need for expert technological skills.

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