COMMERCIAL CRIME
International
November 2018

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

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

IMB NVOCC Register: a business solution to a business problem

THE International Maritime Bureau (IMB) is to launch an initiative that will greatly assist in curbing incidents of false Bills of Lading (B/Ls) issued by non-vessel owning common carriers or NVOCCs.

The Bureau is to launch the IMB NVOCC Register within the next six months. The Register aims to provide a business solution affecting members in the trade chain including banks, ship owners and other stakeholders.

The vast majority of NVOCCs issue B/Ls correctly. There is however a minority that do not. The NVOCC Register aims to provide a mechanism to recognise participating NVOCCs who adhere to a minimum standard of anti-fraud measures in their operations.

The current situation

The IMB verifies many thousands of B/Ls every week for its members and turns around enquiries within a day or two. These B/Ls are based upon shipments from all around the world and they are presented to banks worldwide.

B/Ls are crucial documents relied upon by many stakeholders in the trading chain including banks, shipping companies, carriers, charterers, and others.

IMB's data has shown that 95 percent of the false B/Ls that are identified by the Bureau are issued by or NVOCCs – effectively freight forwarders who take on the responsibilities of a carrier. IMB says that the high prevalence of false NVOCC B/Ls among the volumes checked has been an issue for its member banks for some time. Hence IMB has been asked by the banks to find a way to reduce the incidences of false B/Ls issued by NVOCCs.

"Incidents of ship owners/carriers or their agents issuing B/Ls that are false are rare because they take a big risk in doing so and open themselves to legal action for having issued false documents," says an IMB spokesman.

"However, unlike the carriers or agents, the majority of NVOCCs do not have any assets which are at risk in these transactions except for their reputations."

The spokesman added, "There are many NVOCCs around the world who are highly reputable and who perform their responsibilities to an extremely high standard. But there is a small group who are willing to cooperate with the cargo owners in order to produce documents which benefit the latter to draw out money from the banking system under letters of credit and other instruments."

The IMB spokesman added, "By accepting false B/Ls, banks risk getting into a situation where either there are no cargoes underlying the documents or the shipments may be misrepresented."

"There is also the possibility that the cargoes actually shipped may be of inferior value to what appears on the invoice. These transactions are also used to breach sanctions which has huge implications for the banks involved," the IMB spokesman said.

IMB's solution

IMB is inviting NVOCCs to sign up to its NVOCC Register. In doing so they will also have to sign up to a Code of Conduct for the issuance of B/Ls.

The Code of Conduct requires NVOCCs to keep documentation which confirms the basis on which they have issued a specific B/L. IMB says one of the pieces of documentation that would be required is the master B/L which is issued by the actual carrier.

"The NVOCC B/L has to be uniquely anchored in that master B/L. It must be uniquely linked to the master B/L

Continued on page 3/

In This Issue of CCI

Piracy

IMB advises owners to follow Best Management Practices

INTERNATIONAL Maritime Bureau (IMB) is advising member shipowners to ensure their vessels continue to comply with all Best Management Practices to Deter Piracy and Enhance Maritime Security (BMP5) recommendations, particularly off the coast of Somalia.

In its newly-released third quarter piracy report, IMB says no new incidents have been reported off the coast of Somalia in the first nine months of 2018. However, it cautions that with the retreating of the South West monsoons, this situation may change.

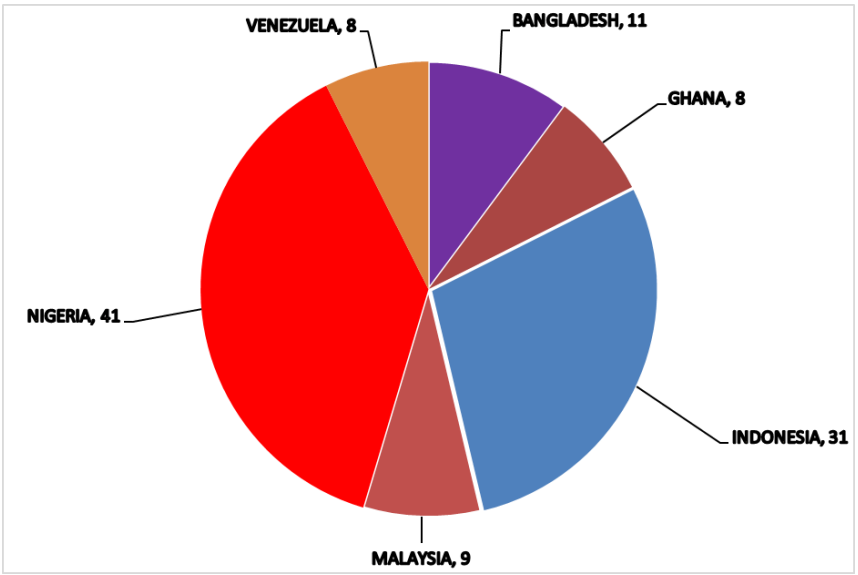
A total of 156 incidents piracy were reported to IMB's Piracy Reporting Centre (PRC) based in Kuala Lumpur in the first nine months of this year compared to 121 for the same period in 2017.

During the 2018 period, 107 vessels were boarded, with 32 attempted attacks. Thirteen ships were fired upon and four vessels hijacked – although no vessels were reported as hijacked in Q3 2018.

This is first time since 1994 when no vessel hijackings have been reported in two consecutive quarters. The number of crew members held hostage in the first nine months of this year rose to 112 seafarers, up from 80 last year and 110 in 2016.

However, the number of crew kidnappings has reduced from 49 in 2017 to 39 in 2018. IMB says 37 of the 39 crew members kidnapped for ransom globally have occurred in the Gulf of Guinea region in seven separate incidents. Twenty-nine crew members were kidnapped in four separate incidents off Nigeria - including 12 seafarers kidnapped from a bulk carrier underway 51nm South West of Bonny Island, Nigeria in September this year. Statistically, the Gulf of Guinea accounts for 57 of the 156 reported incidents. While most of these incidents have been reported in and around Nigeria (41 incidents), the Nigerian Navy has actively responded and dispatched patrol boats when incidents have been reported promptly. There has also been a noticeable increase in the number of vessels boarded at Takoradi anchorage, Ghana.

Six locations that contributed to 69% of total attacks in Q3



"Though incidents in the remaining regions, including some Latin America countries boarder on low level opportunistic theft, the IMB continues to encourage all Masters' and crew to be aware of the risks of this crime and report incidents to its 24-hour manned PRC," IMB says. "The Centre will ensure that the reported incident is relayed without delay to the appropriate response agency and will liaise with the ship, its operators and the response agency until the vessel is deemed safe," IMB added.

**To report an incident to the PRC go to https://www.icc-ccs.org/index.php/piracy-reporting-centre/report-an-incident*

AN attempted pirate attack upon a bulk carrier off the coast of Somalia last month has highlighted the importance of ships following BMP protection measures.

The ship was attacked 340nm off the coast of Somalia in the Somali Basin on October 16. However, due to the application of BMP protection measures by the Master, his crew and the private security team, the piracy attack was thwarted, and the crew and vessel remained safe.

EU NAVFOR said the Master had already evacuated the crew to the citadel when the embarked Armed Security Team responded to the attack. There was a sustained exchange of fire before the skiff with several armed people on board broke off and changed course away from the ship. "Following the collective advice of industry and military counter piracy operations, as written down in BMP5, the Master's actions and the on board security team's reaction proved essential in preventing the suspected pirates getting aboard and seizing the vessel," EU NAVFOR said.

EU NAVFOR's Maritime Security Centre – Horn of Africa also conducted an initial incident assessment and issued an alert and navigation warning to all merchant shipping transiting the area. Several counter-piracy assets of Operation ATALANTA in the Somali Basin were also deployed to maintain heightened vigilance in the area.

IMB Founding Director, Eric Ellen, dies at 88

ICC International Maritime Bureau (IMB) founding Director Eric Frank Ellen QPM has died. He was 88.

Eric served with the organisation from 1981 to 1999 and was instrumental in the fight against maritime crime and piracy.

He started with the Port of London Police from where he retired as Chief Constable in 1980.

He was closely involved with the then International Association of Airport and Seaport Police (IAASP) and believed that sharing of information on crime methods was essential to its prevention and control.

This was also the guiding principle of the IMB in the early years and remains so today.

It was under his leadership that the IMB set up its Piracy Reporting Centre in 1992 based in Kuala Lumpur, which till today remains the only organisation offering a 24-hour and free service for shipmasters to report any piracy, armed robbery or maritime crime.

Eric Frank Ellen

Eric has written numerous papers on different aspects of maritime crime and in his time was a much sought-after speaker at maritime conferences around the world.

Shipping publication Lloyd's List said Eric "leaves a legacy that has benefited the entire industry by bringing a co-ordinated effort to the battle against piracy, hijacking, robbery on the high seas, drug trafficking, stowaways, fraud, and other crimes that cost both money and, some-times, lives."

West Ham United Football Club has lost one of its loyal supporters. Eric will be missed by his family, friends and former colleagues.

from page 1 - IMB to launch NVOCC Register

to stop the situation arising where there are multiple original B/Ls being presented to different banks for payment and other such malpractices," the IMB spokesman said.

The spokesman added that NVOCCs will need to keep a record of those documents, and if at any time the IMB needs to check the authenticity of the issued B/L, NVOCCs are required under the Code of Conduct to provide the backup documents to the Bureau within one working day of being asked.

If they fail to provide a satisfactory explanation of the issuance of the NVOCC B/L, then this would count as a 'strike' against them.

Two such negative strikes in one year of their membership of the Register would result in the IMB writing to them to suggest that they improve their standards of operation and that key people in their company undergo an online course on the issuance of B/Ls and the role of B/Ls.

The NVOCC will also have to show that they have made changes within their operations to ensure that this kind of incident is not repeated.

If they continue to produce false B/Ls in the same year without a proper basis they risk being removed from the Register.

Advantages of staying on the IMB NVOCC Register

IMB says the advantage of NVOCCs staying on the Register is that the banks who process the documents for their customers (who are also the customers of the NVOCC), will process the documents of NVOCCs on the Register faster than those who are not.

It is therefore in the interests of an NVOCC to remain on the Register.

"We hope that traders will encourage NVOCCs to sign up to the Register and the Code of Conduct because it helps the customer process his documents faster. It is a business answer to a business problem.

This initiative aims to raise minimum standards before the regulators step in to take action," the IMB spokesman said.

"The drivers behind this will be the banks and financing institutions who require accountability from the issuers of the documents that they are processing.

"This Register fills that role. We would like to see this being taken up by all NVOCCs who want to see the problem of B/L malpractices stopped," the IMB spokesman stated, adding that the Bureau had received a lot of interest from banks and the International Federation of Freight Forwarders Associations.

Boiler room fraudsters duped more than 170 victims

FIVE men in the United Kingdom have been jailed for a total of nearly18 years for their involvement in a complex boiler room scam that resulted in £2.8 million losses.

A criminal prosecution was brought by the Financial Conduct Authority (FCA).

They duped more than 170 victims into making fraudulent investments. The trial judge said that "some victims lost everything they had" and added that elderly people had been specifically targeted. Their stories "were at times positively heartbreaking."

The men were working in a London based boiler room where they used cold-calling and high-pressure sales tactics to sell worthless and overpriced investments to the public.

Between July 2010 and April 2014, the fraudsters persuaded victims to purchase shares in a company that owned land on the island of Madeira.

The investors were told that the value of the shares would increase substantially when permission to build 20 villas was granted, thereby enhancing the land's value.

Investors were promised guaranteed returns of between 125 percent and 228 percent. None were ever paid.

The FCA says this was one of its largest ever investigations they have ever conducted and dubbed it 'Operation Tidworth'.

It involved:

- 4 separate search operations and one unannounced visit.
- Seizure of over 100 computers and other digital devices.
- 4 million documents and over 1.4 million documents ingested into the FCA's Evidence Management System requiring evidendential assessment and review.
- 142 witnesses.
- 287 witness statements.
- 3,682 exhibits.
- 3 defendants remanded in custody for breach of court bail by committing further offences.

HFW successfully defends IKON

HFW has successfully defended a substantial case of alleged fraud against London-based IKON Finance Ltd and others, originally involving claims of over US$370 million in damages.

In a judgment handed down on 9 October 2018 following a 12-day High Court trial in February and March 2018, Mr Justice Knowles dismissed all the various claims made against the participating defendants in the proceedings, including IKON, bringing the more than two-year dispute to an end. In a summary of the claims, which as originally pleaded had sought over US$370 million in damages, the judge commented that the trial "has appeared to me little more than an elaborate and expensive, unmeritorious and now unsuccessful, attempt to throw off [the Claimants'] responsibility [to their investors] onto the shoulders of the [Defendants]".

The case centred on confirmations of certain "demo" (or demonstration) account balances provided in relation to foreign exchange trading activities being carried out on platforms made available by IKON. The claimants, two private closed-end investment funds, maintained that they understood these confirmations to represent real money, rather than merely virtual money balances.

The claimants alleged that in connection with these confirmations, various of the defendants were liable for dishonest assistance in breaches of fiduciary duty and trust, for unconscionable/knowing receipt, for deceit, and for unlawful means conspiracy.

The judge has ruled that the allegations "fail in every material respect", holding that "there was no dishonesty on the part of the [relevant Defendants]", that "there was no deceit by them", that "nothing they did was relied on by the Claimants", and that "they were not conspirators with [other unrepresented Defendants] or between themselves".

Malaysia investment scam

POLICE in Malaysia have dismantled an investment fraud syndicate with the arrest of 99 people in Kuala Lumpur.

The scam was operated from a luxury office block in Kuala Lumpur but its victims were all from China.

The fraudsters offered a 'stock-broking' service, offering shares to the victims, saying they could get huge returns on their investment in a short time.

The suspects used Voice-Over-Internet Protocol (VOIP) calls to pose as officials before tricking the victims into parting with their hard-earned money.

Initial investigations revealed that the syndicate raked in several million ringgit each month.

Among the items seized by police were 169 mobile phones and 114 laptops. ~ *Source: The Star Malaysia*

Mashreqbank fined US$40m over AML violations

NEW York's Department of Financial Services has fined United Arab Emirates-based Mashreqbank PSC and its New York branch US$40 million for violations of US Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) laws in the New York branch's US dollar clearing operations.

The bank has also been told to hire a third-party compliance consultant to oversee and address deficiencies in the branch's compliance function, including compliance with BSA/AML requirements, federal sanctions laws and New York law and regulations.

"Mashreqbank failed to fully comply with critical New York and federal banking laws aimed at combating international money laundering, terrorist financing and other related threats by failing to provide adequate oversight of transactions by customers in high-risk regions," Financial Services Superintendent Maria T. Vullo said.

DFS conducted a safety and soundness examination of the New York branch's operations in 2016, finding that the branch had been unable to meet its commitments to improve its compliance function sufficiently.

Following this examination, DFS examiners issued the branch a low overall score, whereas two years earlier the New York branch had received a satisfactory score on its safety and soundness examination.

This downgrade was the result mainly of deficiencies in the New York branch's Bank Secrecy Act and Anti-Money Laundering program, as well as certain defects identified in its program and policies designed to comply fully with Office of Foreign Assets Control (OFAC) regulations.

At the time of the 2016 Examination, the branch's BSA/AML and OFAC policies lacked detail, nuance or complexity, doing little more than citing standard language from applicable regulations.

Subsequently, in November and December of 2017, DFS examiners, along with examiners from Federal Reserve Bank of New York, conducted a joint examination. Examiners found that records regarding specific alerts and dispositions continued to lack detailed infor-mation, making it difficult for examiners to assess the adequacy of investigations conducted by compliance staff. Rationales for closing alerts also failed to include essential information.

Further, the examination found that each transaction monitoring alert would be reviewed only once by a single reviewer, who would then determine whether the alert should be closed or escalated, but without adequate quality assurance reviews.

The branch's OFAC program also suffered from certain deficiencies in important aspects of its recordkeeping. The branch maintained inadequate documentation concerning its dispositions of OFAC alerts and cases, with branch compliance staff failing to properly substantiate its rationales for waiving specific alerts and cases.

The joint examination also found that the bank's Head Office failed to provide sufficient oversight of a third-party auditor hired to conduct the branch's 2017 AML/BSA audit and to evaluate the branch's remedial work.

The 2017 examination detailed additional deficiencies and assigned the New York branch another low score for the second consecutive examination cycle, which followed the branch's earlier failures to fully remediate compliance issues.

THE Heads of Financial Intelligence Units (FIUs) have approved a set of indicators for corruption related cases which can be used as a tool to help identify transactions and clients related to the money laundering of the proceeds of corruption.

This took place at the 25th Egmont Group Plenary in Sydney, Australia which saw 419 delegates (including 23 observers and international partners). The Group agreed to continue to update the list of indicators through engagement with the private sector. On public-private partnerships (PPPs) members recognised the importance of private and public sector cooperation to harness collective capabilities in the joint fight against financial crime.

Addressing the topic from the perspective of FIUs, the plenary discussed the many contexts, opportunities, and challenges FIUs face when participating in PPPs. The gathering agreed that PPPs can, in a number of juris-dictions, enhance the quality of repor-ting, improve the expertise and know- ledge of all partners as well as provide more flexibility and agility to respond to the fast-changing ML/TF threat environment. It also acknowledged the legislative, technological, and cost barriers that can exist in the formation of public-private partnerships.

The FIUs of Azerbaijan, Benin, the Republic of Congo and Zambia were welcomed as new Egmont Group members following endorsement by the Heads of FIU. The Group's membership now stands at 159 FIUs.

Corruption/Bribery

Zimbabwe takes steps towards fighting commercial crime

THE POLITICAL career of Zimbabwe's longtime President Robert Mugabe may have been consigned to history last November (2017), when he was forced from power, but the patronage system and corruption of his 38-year rule in Zimbabwe continues to be felt, both on the streets and in boardrooms. Kudzai Mashininga *reports from Harare*.

WITH the newly-elected Zanu-PF government of President Emmerson Mnangagwa consolidating its power after a contested election on July 30, it faces an uphill task to restore confidence that Zimbabwe's public authorities are serious in tackling commercial crime.

This is because, in this potentially wealthy southern African country, fighting graft, fraud, and business rule breaking is not just about making sure the police do their job well (although that would help). It is first and foremost making sure that the formal economy operates efficiently in Zimbabwe.

Without this, the country's 16 million people will continue to rely on the informal black-market economy that has effectively staved off ruin as Mugabe entrenched his personalised and often arbitrary rule.

Collusion

Daisy (not her real name), a Zimbabwean illegal immigrant living in in neighbouring South Africa, is a perfect example of the kind of professional woman who could thrive in a legal business in her home country, if it were run properly.

Instead, she makes a living by running an illegal forex exchange business at the South Africa-Zimbabwe border.

Daisy provides Zimbabwe bond notes (a local auxiliary currency for a country that has used the US dollar as its main unit of money since 2008) to travellers at the border, usually in exchange for South African Rands and US dollars, at profitable rates compared to those she used to source bond notes.

She has a willing market of buyers because Zimbabwe's banks are short of these bond notes and indeed US dollars, leaving most Zimbabweans no option but to buy bond notes from street money changers such as Daisy.

Legal *bureaux de change* are shunned in Zimbabwe, because the government insists that they charge US$1 for each bond note, far more expensive than on the black market. The result is that Daisy and her buyers are technically committing commercial crimes, just to live.

Moreover, there is collusion with bankers: "We work with some bank managers to get money out. Moving it across the border is not a problem. You only have to know the right people at the border and no questions would be asked," she told *Commercial Crime International*.

Faltering banking sector

Of course, such informal money flows are ripe for exploitation by real criminals who harm people, like mobsters, corrupt officials and scammers, who may want to move ill-gotten gains out of Zimbabwe to be laundered abroad.

Such movements of cash across Zimbabwe's borders have been identified by the Eastern and Southern Africa Anti Money Laundering Group (ESAAMLG), an African organisation that works to combat money laundering thro-ugh peer review mutual evaluation processes.

In its latest report on Zimbabwe (released in September 2016), ESAAMLG said the country's faltering banking sector had been identified as the most exposed to risks of money laundering, and – through its inefficiency – unable to combat this crime. The report said individuals physically carry cash across the borders while legal entities transfer funds to foreign jurisdictions using personal or non-business accounts to avoid detection.

Since coming to power in November after Mugabe was pushed out by his erstwhile military allies, President Emmerson Mnangagwa has however started trying to combat dirty money flows.

In July, a new Money Laundering and Proceeds of Crime (Ammendment) Act was passed by Zimbabwe's parliament and Mnangagwa has since launched an anti-graft campaign, arguing that it and practical law enforcement policies to follow will help turn Zimbabwe into a middle-income country that is corruption free by 2030.

Action taken

There certainly has been some action. Since Mugabe's resignation, a number of former powerful political figures have been arrested for corruption and charged, their cases pending before the courts.

These include Mugabe-era political leaders such as former home affairs minister Ignatius Chombo, past energy minster Samuel Undenge, ex-mines minister Walter Chidhakwa, toppled local government minister Saviour Kasukuwere as well as (last month – September), Shuvai Junior Gumbochuma, sister to the country's once powerful First Lady Grace Mugabe, accused of reselling state land for personal profit.

Also, days after coming to power, Mnangagwa also gave a three-

Continued on page 7/

from page 6 - Zimbabwe moves to tackle corruption

month amnesty to Zimbabweans who had exported forex – illegally - to repatriate this money without facing questions or prosecution. This tactic was not very effective - official figures from the Reserve Bank of Zimbabwe indicate that while US$1.4 billion's worth of forex had been moved from Zimbabwe during the period just before Mugabe was toppled, just US$5.91 million was repatriated during the amnesty period.

Meanwhile, the new President has told his new ministers to publicly declare their personal assets. The Parliament has developed a declaration form that all MPs must submit within 30 days of taking an oath of office and in Zimbabwe all ministers are also Members of Parliament.

Mnangagwa also fired the country's Mugabe-era Prosecutor General Johannes Tomana for allegedly not acting upon corruption allegations and appointed an acting Prosecutor General Kumbirai Hodzi, who was formally appointed to the position in July.

Prosecuting crimes

In an interview with *Commercial Crime International*, Hodzi said he has started moving forward to prosecute commercial crimes and corruption cases, carrying out a post-mortem of the challenges faced by Zimbabwe's Attorney General's Office.

"With high profile cases, we now allocate a minimum of three trial prosecutors per case to improve presentation of cases in court, to ensure that there is adequate evidence to secure conviction," he said.

He added that the government has also raised the salaries of prosecutors to reduce the temptation of accepting bribes to drop or impede cases.

"We have also revamped the Special Offences Unit which deals with cases such as money laundering, fraud and misrepresentations to ensure that the unit meets the current demands. This has been done through retraining of officers, transfers and reorganising and ensuring that the unit has adequate resources," said Hodzi.

He is also lobbying for the decentralisation of special anti-corruption courts to cover more areas of the country. Hodzi said his office is setting up an Asset, Seizure and Forfeiture Unit seeking to take control of ill-gotten funds associated with any convictions, including funds stashed in international banks.

"We also have a programme to protect whistleblowers," he added.

Specialist commercial court

The Confederation of Zimbabwe Industries (CZI) said there is hope that law enforcement is improving from its woeful Mugabe-era reputation when citizens were of the opinion that reporting crimes was pointless because no action was taken.

"We have requested for a separate commercial court. We are expecting a major shift from the new government on the issue of prosecution," he said. Commercial crimes were left festering and business could not afford to combat such wrong-doing itself: "In the past people ended up not reporting on issues of commercial crimes because they were taking too long to be resolved," said CZI president Sifelani Jabangwe.

"The current champions [of reforms] all have clouds of corruption hanging above their heads," Zimbabwean public administration expert Ricky Mukonza

The Zimbabwe Anti-Corruption Commission did not respond promptly to inquiries from *Commercial Crime International*, but in September its head of investgations Goodson Nguni told Zimbabwe state media that the graft watchdog had recently established a special Economy and Trade Unit to investigate fraud, tax violations and "economic sabotage" in the public and private sectors. He said the unit consists of 10 lawyers, auditors, accountants and investigators.

Nguni said the Anti-Corruption Commission was also following up on people who had not complied with the President's amnesty to return forex.

He said they were receiving support from the new administration and there was no longer political interference with their work, which was the case during Mugabe's rule. Nguni said the Commission would soon be hiring more staff and opening provincial offices.

Areas that are lacking

Will these reforms work? Zimbabwean public administration expert Ricky Mukonza, a senior lecturer at South Africa's Tshwane University of Technology, said time will tell.

"What is lacking in the current fight against crime are independent institutions that are genuinely fighting the undesirable scourge. Another aspect that is lacking are acceptable champions of the cause.

Continued on page 8/

from page 7 – Zimbabwe corruption reforms

"The current champions including the country's leadership, all have clouds of corruption hanging above their heads," he said.

A key problem is that "nothing has been done to known or suspected Zanu-PF leaders engaged in corruption who are in President Mnangagwa's corner," his supporters in the factional battle that ousted Mugabe.

"One is left wondering whether this is a genuine war on corruption or it is an attempt to settle political scores disguised as a war against corruption," he said.

The chairperson of the Zimbabwe chapter of the African Parliamentarians Against Corruption (APNAC) Willias Madzimure said his organisation was pushing Zimbabwe MPs to declare assets.

But he said pressure for this to happen was lacking: "The institutions that are meant to fight crime are weak and poor funded. They also lack independence and capacity. There is need for strong institutions, including Parliament," he said.

"Another thing that needs to be addressed is that Zimbabwe has several laws to fight commercial crimes, money laundering and corruption that are scattered everywhere.

"These laws need to be harmonised. Institutions that preside over these pieces of legislation must be well equipped and trained. Best practices must be learned."

MACN boosts membership to over 100

MAJOR shipping lines ZIM and Frontline have become members of the Maritime Anti-Corruption Network (MACN), boosting the organisation's membership to over 100 companies across the maritime sector.

MACN said its members now represent a major percentage of the global world fleet by tonnage and play a key role in ocean transport and global logistics.

MACN Chair, John Sypnowich, said, "As an industry led organisation, we have strength in numbers. By having more and more companies join our cause, we have a better and better chance of making a difference and eliminating all forms of corruption. Together, as an industry, we are taking a stand."

MACN Programme Director, Cecilia Müller Torbrand, said MACN has received over 25,000 anonymous reports of corrupt demands to-date. Only last year MACN received over 260 anonymous incident which were directly related to the safety of crew.

"It is a problem that is too-often excused as being too hard to solve – 'it is the way things have always been done'. While the shipping industry is not alone in facing this enormous problem, we have shown unparalleled leadership in spearheading business-led anti-corruption efforts," she said.

"The stronger our membership, the greater the impact of our collective actions. Shipping companies, working together to refuse corrupt demands, have undertaken projects in Nigeria, Argentina, Indonesia, and Egypt. Our 'Say No' campaign in the Suez has been a particular success. This has shown that as an industry we can fight corruption and win. And we can do this better than anyone," she added.

Man bribed bank manager

A man was sentenced to four months' in prison in Hong Kong after admitting that he had offered a bribe of HK$100,000 to an employee of a bank to assist him in opening a corporate account.

He was charged by the Independent Commission Against Corruption (ICAC) and a court heard that at the material time, the defendant was the chief executive officer and sole director of a company engaged in crude oil trading business.

In late July 2018, DBS Bank (Hong Kong) Limited (DBS Bank) received an online application from the defendant for opening a corporate account for the company. The bank assigned a senior relationship manager to handle the application.

In August 2018, the defendant was asked to provide supplementary documents in support of his application. Having examined all the documents submitted by him, the manager rejected the application due to insufficient details to prove the company's business.

The court heard that on 17 August 2018, the manager received two emails and a text message from the defendant in which he urged the former to assist him in opening a bank account and a sum of HK$ 100,000 would be given as a reward. The manager reported the matter to her supervisors.

DBS Bank had rendered full assistance to the ICAC during the investigation.

Munich Re launches SME cyber coverage solution

MUNICH Reinsurance America, Inc. (Munich Re) has launched a reinsurance solution for regional property/casualty insurance carriers seeking to provide cyber coverage and associated services to their small and medium-size enterprise (SME) clients.

Munich Re's cyber solution provides reinsurance capacity for limits up to US$15 million, including technical expertise, and tools such as a risk management portal and a post-breach services panel to primary insurance carriers that may not have the experience or resources necessary to provide cyber protection to their clients.

Image: Pixabay

A May 2016 IBISWorld industry report noted that 72 percent of US cyberattacks occurred in SMEs.

"Cyber events are a growing threat to businesses of every size," said Annamaria Landaverde, vice president and head of cyber for the US Reinsurance Division, Munich Re.

The product offers regional primary carriers a flexible, turnkey cyber solution, including providing coverage for a loss resulting from a variety of events, such as a denial-of-service attack, unauthorised access, introduction of malicious code, privacy breach, extortion threat, regulatory proceedings, and/or third-party claims.

Munich Re said insurance carriers participating its cyber solution will retain a portion of the risk. It added, the solution can include ISO's stand-alone commercial cyber policy or the information security protection cyber policy as well as a primary carrier's proprietary cyber product.

"We are pleased that Munich Re has recognized ISO's cyber insurance program as part of its turnkey solution, as our program can provide primary carriers with an array of coverage options to help address the growing and diverse cyber market," said Maroun Mourad, president of ISO Commercial Lines.

"That's important because cyber risk is constantly changing and presenting significant challenges for those looking to insure the wide range of small and midsize businesses in need of coverage."

BIMCO survey says shipping needs to be better prepared

A cyber security survey by BIMCO has shown that the shipping industry needs to be better prepared in the future to guard against attacks.

According to the survey, in which more than 350 individuals responded, more than a fifth reported that they had been the victim of an attack.

In addition, 72 percent said that their own company was a victim of a cyber related incident in the last 12 months.

BIMCO said that 49 percent of respondents reported service disruption as the result of the attack and the incident caused financial loss for 25 percent of respondents. Only 16 percent had the breach covered by insurance while 84 percent did not have the attack covered.

"The many cyber related attacks and incidents within the last 12 months indicates that there is still good reason for the industry to be better prepared in the future," said BIMCO's Head of Maritime Technology and Regulation, Aron Frank Sorensen.

"In the survey, 27 percent of respondents reported that they had never received cyber security training, and only about half of respondents have a business continuity plan in place, should they become a victim of a cyber security attack, while 31 percent of respondents had none," he added.

BIMCO and Fairplay launched the annual survey for the third time in June with the aim to gather insight and greater awareness on how the industry prepares for and handles cyber attacks.

The survey showed that the Industry guidelines initiated by BIMCO on cyber security were the most widely used by respondents.

"That is very encouraging, but it also pushes us to improve our guidelines. The survey matters because it allows us to gather knowledge about cyber risks and attacks that would normally never be reported.

"We can use the result to further develop the cyber security guidelines and thereby help the industry to be more prepared and better protected in the future," Sorensen said.

Cyber risk in finance and banking: size does not really matter

CYBER risk in finance and banking firms is more consistent regardless of the size of those companies, according to an assessment released by the US Chamber of Commerce and FICO which aims to benchmark cybersecurity risks across key industry sectors.

The Assessment of Business Cybersecurity (ABC) found that large companies are at greater risk than their smaller counterparts, and that cybersecurity risk is correlated to both the size of the organisation and the complexity of their networks.

However the correlation of size and risk is less pronounced in the finance and banking sectors as well as the health care sector.

These sectors have lower variability across companies of different sizes compared with the variability in other sectors, and the variance across all sizes of firms in these sectors is more than 40 percent lower than the overall variance across others.

Interestingly, companies in these two sectors are custodians of especially valuable personally identifiable information and are subject to specific compliance regimes regarding data protection (the US' Health Insurance Portability and Accountability Act of 1996) and the Payment Card Industry Data Security Standard, respectively).

The ABC said the smaller difference in relative risk across size bands in this group appears to be attributable to more consistent external risk (more consistent targeting of these companies by threat actors) and better security controls being applied by security teams regardless of the scale of organisational assets.

Overall, the assessment found that;

- Large companies are at greater risk than their smaller counterparts. Cybersecurity risk is correlated to both the size of the organisation and the complexity of the organisation's networks. Larger networks are more difficult to manage and tend to increase the forward-looking odds of a breach incident.
- The relative risk of industry sectors varies widely. The highest-scoring sector was construction at 764, while the media, telecommunications and technology sector scored lowest at 619 - this difference represents nearly 200 percent variance in odds of significant cyber incident.
- The risk performance differentiation between large and small entities is less pronounced in industries with the most sensitive data, such as health care and finance and banking, where companies are subject to specific compliance regimes.

The ABC is based on scoring more than 2,500 US companies using the FICO Cyber Risk Score for assessing cybersecurity risk.

Control deficiencies left Tesco Bank vulnerable

THE United Kingdom's Financial Conduct Authority (FCA) has fined Tesco Bank £16.4 million for failing to exercise due skill, care and diligence in protecting its personal current account holders against a cyber attack.

The cyber attack took place in November 2016.

FCA said cyber criminals exploited deficiencies in Tesco Bank's design of its debit card, its financial crime controls and in its Financial Crime Operations Team to carry out the attack.

Those deficiencies left Tesco Bank's personal current account holders vulnerable to a largely avoidable incident that occurred over 48 hours and which netted the cyber attackers £2.26m.

Following the attack, Tesco Bank immediately put in place a comprehensive redress programme and devoted significant resources to improving the deficiencies that left the bank vulnerable to the attack and instituted a comprehensive review of its financial crime controls.

It has made significant improvements both to enhance its financial crime systems and controls and the skills of the individuals who operate them.

Tesco Bank provided a high level of cooperation to the FCA. Through a combination of this level of cooperation, its comprehensive redress programme which fully compensated customers, and in acknowledgment that it stopped a significant percentage of unauthorised transactions, the FCA granted the bank 30 percent credit for mitigation.

In addition, Tesco Bank agreed to an early settlement of this matter which qualified for a 30 percent (Stage 1) discount under the FCA's executive settlement procedure.

"But for the mitigation credit and the Stage 1 discount, the FCA said it would have imposed a penalty of £33.6 million," the FCA said.

Europol report reveals cybercrime trends and developments

MEMBERS may want to take note of Europol's latest cybercrime report which provides insights into emerging threats and key developments.

The organisation's fifth annual Internet Organised Crime Threat Assessment (IOCTA) says cybercriminals are adopting creative new techniques to target their victims at an unprecedented pace and are constantly seeking methods to avoid law enforcement detection.

It describes the now common method where cybercriminals offer "off-the-shelf" cyber-attack services or products to enable low-level cybercriminals to carry out high-level attacks.

Europol sheds some light on some of the main trends here. A complete overview can be found in the full report on Europol's website.

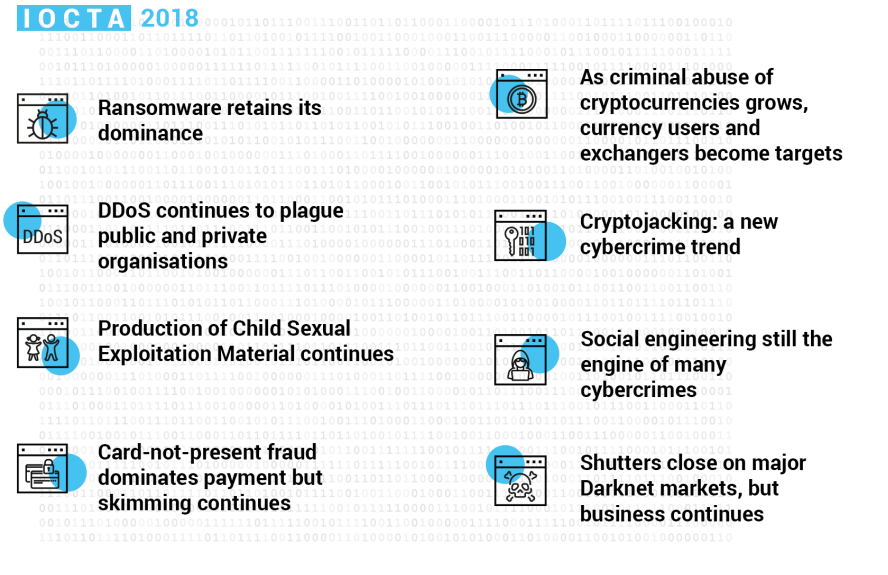


Image: Europol

RANSOMWARE MALWARE, BEWARE!

- Ransomware has become a standard attack tool for cybercriminals. However, criminals are moving from random attacks to targeting companies or individuals where greater potential benefits lie.
- Mobile malware may grow as users shift from online to mobile banking.
- Cyber attacks have become increasingly stealthy and harder to detect. Attacks using fileless malware have become a standard component of the crime-as-a-service industry.
- The GDPR legislation requires breaches to be reported within 72 hours. Criminals may try to extort breached organisations. While this is not new, it is possible that hacked companies will prefer to pay a smaller ransom to a hacker for non-disclosure than the steep fine that might be imposed by the authorities.
- The motive behind network intrusions is the illegal acquisition of data, for a variety of purposes, including phishing or payment fraud.
- Distributed-Denial-of-Service (DDoS) attacks continue to grow and tools to launch them are easily available as a service, allowing unskilled individuals to launch significant DDoS attacks.
- Continued growth in the volume of social engineering attacks is expected, but as a key component of more complex cyber attacks. West African fraudsters are likely to have a more significant role within the EU in the future, as Africa continues to have the fastest growing internet usage globally.

CRYPTOCURRENCIES ARE NO SAFE HAVEN

- Criminals will continue to abuse cryptocurrencies. Cyber attacks which historically targeted traditional financial instruments are now targeting businesses and users of cryptocurrencies.
- Cryptomining has been exploited by financially motivated cybercriminals, who for instance hack legitimate websites to cryptojack users visiting those sites. Such attacks are much more appealing to cybercriminals wishing to keep a low profile, requiring little or no victim engagement and, at least currently, minimal law enforcement attention (with browser-based mining not actually being illegal).
- Another emerging threat is 'true' cryptomining malware which uses the processing power of infected machines to mine cryptocurrencies.
- Europol anticipates a more pronounced shift towards more privacy-oriented currencies. An increase in extortion demands and ransomware in these currencies will exemplify this shift.

PAYMENT CARD FRAUD

- Skimming is still successful as card magnetic stripes continue to be used. Instant payments may reduce detection and intervention opportunities by banks, potentially leading to higher fraud rates. Telecommunications fraud involving non-cash payments is growing.

* *Source: Europol*

Cybercrime

UK banks ink MoU with European Cyber Centre

EUROPOL'S European Cybercrime Centre (EC3) have signed a Memorandum of Understanding (MoU) with the Cyber Defence Alliance Limited (CDA), a group of British-based banks and law enforcement agencies which work together to share intelligence and fight against hackers and fraudsters.

The purpose of this agreement is to address cyber threats affecting the banking and financial sector by organising activities, exchanging expertise such as best practice, statistical data, technical information or trends related to cybercrime and cooperating with each other when implementing projects.

The MoU was signed by Maria Vello, CEO of the CDA and Steven Wilson, Head of EC3, during a visit to the Europol headquarters in The Hague.

Photo: Europol

Wilson said, "The Cyber Defence Alliance is a valuable partner for the EC3 and the signing of this MoU illustrates the logical next step in our mission to jointly tackle the threat of cybercrime. CDA does important work in facilitating the sharing of information on cybersecurity incidents and is thus an essential partner in securing the global digital space."

Vello said, "For us, EC3 is an invaluable strategic partner and critical to our quest to fight cybercrime and threats collectively and collaboratively across Europe and globally.

"EC3 adds a whole new dimension to the CDA to help enable our mission and to take a proactive approach to tackling cybercrime at all levels of this miscreant ecosystem of shared criminal services."

Fraudsters bought compromised corporate credit cards online

FRAUDSTERS bought airline and train tickets using compromised corporate credit cards and credentials, which they purchased online from other criminals offering them for sale – known as 'crime-a-service' business model.

Law enforcement authorities have identified that the cyber criminals made 493 fraudulent bookings. In most cases the tickets were one-way tickets from Beirut to European Member States.

Following police operations, two people have been arrested in a series of coordinated raids across Germany and Sweden. House searches were carried out where police recovered some €54,000 and US$55,000. The arrestees are believed to be the key organisers of a cyber fraud gang.

The fraud was brought to the attention of law enforcement by the private sector highlighting once again how instrumental public-private partnerships are in fighting this type of fraud. Europol and the European Border and Coast Guard Agency (Frontex) have jointly identified significant crossovers between payment card fraud and irregular migration and trafficking in human beings, leading to a number of arrests in recent years.

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