COMMERCIAL CRIME International

May 2018

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

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

Stay alert to Brazilian Global Bonds fraud

MEMBERS are being warned about an elaborate fraud involving Brazilian Global Bonds that has come to the attention of CCS' Financial Intelligence Bureau which has resulted in the victim losing around $200,000.

The scam, a classic case of advanced fee fraud, involved several individuals and saw the perpetrators claiming to have the backing of top banking executives and that the 'documents' had been approved by several major international banks.

The victim, the owner of an aviation leasing company, was approached in late 2016 by an individual who said he was an investor and wanted to buy the victim's business.

The individual said he owned a Brazilian Global Bond (through his company) and appeared to provide proof by supplying some documents to that effect.

The victim was asked for an advanced payment of US$70,000 to collateralise the bond, and the perpetrator promised that the process would take just a few days and that it was risk-free.

This was done but time went by and nothing materialised, with the perpetrator coming up with many reasons as to why the deal was delayed.

In early 2017, another individual purporting to be a partner of the investor approached the victim, promising that they could help speed up the collateralisation process through a company (Company A), but that he would need $25,000 to do this, which the victim handed over.

Over the next few weeks the victim had several email communications between this second individual and the 'president' of Company A, but this too stopped eventually.

When confronted by the victim, they apologised and said that a few things had gone wrong and that the victim would be reimbursed as soon as possible. Till today, no repayment has been made.

In late 2017, the initial investor introduced the victim to another man who was described as being a 'good friend', and a very well-known and respected businessman, who had closed many financial deals.

The victim met this man, who further claimed to be a representative for some bankers from the Central Bank of Brazil. He offered to assign to the victim's company some Brazilian Global Bonds, but again said he needed to be paid to help monetise the bonds.

Over the course of four months, till early this year, the victim made several payments to company bank accounts and to one personal account.

During this time, and in yet another twist to the scam, the initial investor now said that the bond had expired and that he would need more money to set it up again. The victim paid him an agreed amount.

The victim was also introduced to another 'friend' of the investor, supposedly an expert in dealing with securities, who would help keep the projects on track.

He was also shown documents allegedly from major international banks, all verified by the expert as being genuine. He was further introduced to someone who was said to work for the Central Bank of Brazil. This individual would be in charge of assigning the bonds to the companies.

In order to make the scam appear legitimate, the victim was also taken to meet a top executive of the global markets division at an international bank.

Continued on page 3/

In This Issue of CCI

Piracy

Gulf of Guinea warning as variation seen in attacks

THE latest piracy report by International Maritime Bureau (IMB) will not make easy reading for shipowners whose ships ply the Gulf of Guinea region, as attacks show there is no let-up in this hotspot.

In Q1 2018, globally, the IMB's Piracy Reporting Centre received reports of 66 incidents. This was up from 43 for the same period in 2017, and 37 in Q1 in 2016. Worldwide in the first three months of this year, 100 crew were taken hostage and 14 kidnapped from their vessels.

The Gulf of Guinea accounts for 29 incidents in Q1 2018, more than 40 percent of the global total. Of the 114 seafarers captured worldwide, all but one were in the Gulf of Guinea.

A total of 39 vessels were boarded, 11 fired upon and four vessels hijacked. IMB received a further 12 reports of attempted attacks. "The hijacking of product tankers from anchorages in the Gulf of Guinea is a cause of concern," says an IMB spokesperson.

All four vessel hijackings were in the Gulf of Guinea, where no hijackings were reported in 2017. Two product tankers were hijacked from Cotonou anchorage in mid-January and early February, prompting the IMB PRC to issue a warning to ships.

Towards the end of March, two fishing vessels were hijacked 30nm off Nigeria and 27nm off Ghana.
The recent hijackings indicate a change in pattern to those previously seen in the area. In previous cases, product tankers were hijacked, taken to international waters, rendezvous with smaller vessels and the cargo discharged. The vessel would then normally be returned.

"The recent attacks see a slight refinement. As seen in the Cotonou incidents, the ships were taken from anchorage, sailed out under the control of pirates into international waters (and in one case, the cargo was stolen)," said the IMB spokesperson.

"However, in both these cases, before the pirates left, they kidnapped some of the crew members. The crew were eventually released, after a payment of a ransom. Worryingly, in the second case they did not even take the cargo. We have also seen this happening with reefer vessels and fishing vessels in international waters and the south of Nigeria – where crew were kidnapped, and the vessel released," the spokesperson added, clearly showing that the pirates' intent is to steal the oil cargo and kidnap crew.

IMB says ships at anchor can be and should be monitored by port authorities, and any unauthorised movements in the anchorage area should raise the alarm.

"This will enable local law enforcement to intervene and could prevent an attack. Furthermore, it is also unlikely that the pirate gangs are able to operate without some infrastructure ashore, because they will need somewhere to store boats and weapons for easy retrieval. All of these are pinpoints which can be monitored and controlled," IMB said.

IMB however gave credit to authorities' law enforcement agencies in Benin, Togo and Nigeria who were quick to respond and sent ships out to the scene of attacks when alerted by IMB. Their presence has prevented attacks from escalating.

As always IMB PRC is advising ships to be vigilant and adhere to the industry and the International Maritime Organization recommendations on anti-piracy.

Ships are also advised to report all actual and attempted attacks and suspicious sightings to the IMB PRC.
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

NatWest: Eight scams to watch out for

A new report from NatWest has identified the top ways they expect fraudsters will try and get their hands on people's cash in 2018.

NatWest has worked with research agency The Future Laboratory to analyse data from the last 18 months to predict eight frauds expected to emerge in 2018.

Eight scams to watch out for in 2018

Social media spying
People might not realise how much information they are giving away, but to a fraudster the posts can be very helpful in setting up a scam.

Malicious software on smartphones
It is expected that malware or malicious software threats will grow among mobile devices.

Bogus Brexit investments
Consumers should be wary of fake investment opportunities. For example, fraudsters may email customers, warning Brexit will affect their savings, and that they urgently need to move them into a seemingly plausible, but actually fake, investment product.

Fraudsters preying on World Cup excitement
Some fraudsters will sell football tickets that are either fake or will never arrive. It is also expected that "package trips" will be offered by fake travel companies. Always buy tickets from a reputable source.

Money mules
Mule recruiters may trawl social media for potential targets, particularly cash-strapped students in university towns, and use them to inadvertently launder money. Money mules receive the stolen funds into their account, they are then asked to withdraw it and send the money to a different account, often one overseas, keeping some of the money for themselves.

Wedding excitement
Experts fear couples could be easy prey for fraudsters who tempt victims with extravagant offers at bargain prices. Fraudsters can set up fake websites for elements of the big day like venue hire, catering, or wedding dresses that appear very realistic. Fake wedding planners will take people's money and then disappear.

Romance scams
Criminals create fake profiles to form a relationship with their victims. They use messaging to mine victims' personal details to use for identity fraud. Or, just when the victim thinks they have met the perfect partner the fraudsters asks them for money.

Scams aimed at first-time buyers
Computer hackers monitor emails sent by a solicitor to a first-time buyer and then they pounce, pretending to be the solicitor and telling them the solicitors' bank account details have changed in order to steal cash.

Julie McArdle, NatWest security manager said: "Scammers are dogged in their attempts to get their hands on people's money and are always looking for new ways to get ahead. This means banks and customers need to evolve alongside scammers too."

from page 1 - Brazilian Global Bonds fraud

In February, the victim discovered that the individual who supposedly worked with the Central Bank of Brazil did not exist and that email communications from the various parties had all originated from the same IP address.

The victim also met alone with the executive of the international bank a second time, where he was told that the fraudsters had been trying to open a bank account at the bank.

FIB, upon examining the documents, was able to spot several red flags that if seen earlier, could have been a warning and prevent considerable losses.

"Members must be aware that while fraud cases like this one and others are directed at non-banking victims, eventually these funds will turn up in a bank account," said a FIB spokesman.

"Banks should, as always, carry out due diligence and Know Your Customer checks including asking about the purpose and source of the funds and what is the business of the customer. If they don't, they could be assisting in the laundering of criminal proceeds," the spokesman added.

FIB said cases such as these show that fraudsters are actually successful in carrying out these scams and that these were not mere 'phishing' expeditions.

In all these cases, the alertness of banks is vital to stop the fraud from further continuing, as seen in the case of Luis Nobre, when a bank stopped an account containing €88 million after growing suspicious about the nature of the transactions.

Oil and gas executives defrauded investors

THE Securities and Exchange Commission has charged a Dallas-based oil-and-gas company and two of its executives with defrauding investors out of at least $950,000 through a string of fraudulent oil-and-gas securities offerings.

The SEC's complaint, filed in federal court in the Northern District of Texas, alleges that SA used his company, Americrude, Inc., to defraud multiple investors in seven securities offerings that purportedly raised funds to acquire working interests in oil-and-gas prospects.

The SEC alleges that Americrude, SA, and DW, who was Americrude's nominal President, used a combination of cold calls, high-pressure sales pitches, and false and misleading statements to lure investors into Americrude's fraudulent offerings.

The defendants misrepresented Americrude's track record, the reserve potential of its oil-and-gas prospects, and its intended use of proceeds from the offerings.

SA is also alleged to have used an alias to conceal his involvement in the offering fraud and to hide his

Image: Pixabay

prior felony convictions from potential investors.

According to the complaint, while investors only received back approximately $2,500 of their principal, Americrude and SA misused and misappropriated more than $196,000 of investor funds, which were allegedly spent on, among other things, retail and entertainment expenses.

Americrude, SA, and DW are charged with violating the Securities Act of 1933 and the Securities Exchange Act. Additionally, DW is charged with violating the Exchange Act based on his alleged role as an unregistered broker.

The SEC encourages investors to check the backgrounds of people selling investments by using the SEC's investor.gov website to quickly identify whether they are registered professionals and confirm their identity.

FIB International Financial Crime Forum

CHANGING technology and its implications on compliance policies, Shariya banking, artificial intelligence solutions in identifying financial crime, cybercrime, digital money and cryptocurrencies and the challenge these bring for anti-money laundering regulation and compliance will be among the main topics discussed at the 13th ICC FIB International Financial Crime Forum.

Organised by ICC Financial Investigation Bureau (FIB), the Forum will be held in Kuala Lumpur on July 18 and 19.

"The Forum will look at practical approaches to identifying and tackling the potential pitfalls faced by those using financial instruments within international banking and financial services," a FIB spokesman said.

"The unique approach of this specialist interactive Forum presents delegates from around the world with the latest fraud trends and developments, and assists them in dealing with financial crime, money laundering and counter terrorism financing issues."

FIB said the Forum also provides delegates the opportunity to gain awareness on the changes being affected due to technological innovations.

It is ideal for those from financial sector institutions such as national FIU's, international bank compliance and risk departments, regulators, lawyers, accountancy firms, stock brokers and law enforcement agencies.

Other main topics include;

- Banking governance in the new era
- Multiple jurisdictions - legal challenges
- Red Flags in fraudulent documents
- Insolvency and fraud – tracing and recovering losses

Members are urged to attend the Forum. Group discounts are available.

To register your interest, go to www.icc-ccs.org/KL2018

Or Contact: Cyrus Mody (cmody@icc-ccs.org)
ICC Commercial Crime Services
Cinnabar Wharf,
26 Wapping High Street, London.
E1W 1NG United Kingdom.

Telephone: +44(0)207 423 6960

Fax: +44(0)207 423 6961

Email: FIB@icc-ccs.org

Iceland needs to boost AML/CFT regime

ICELAND needs better internal cooperation and coordination to effectively tackle money laundering and terrorist financing, according to the Financial Action Task Force (FAFT).

The FATF conducted an assessment of Iceland's anti-money laundering and counter-terrorist financing (AML/CFT) system. It is a comprehensive review of the effectiveness of Iceland's AML/CFT system and its level of compliance with the FATF Recommendations.

FAFT said between 2008 and 2015, Iceland demonstrated a high level of cooperation and coordination as they focused almost exclusively on the financial crimes and complex cases surrounding the 2008 banking collapse. However, it said this did not extend to anti-money laundering and counter terrorist financing, which has not received sufficient attention as a result.

"Icelandic authorities have a fragmented understanding of AML/CFT risks, which is not used for further policy development. Although supervisors are beginning to identify areas of risk relevant to their sectors, they need to further enhance their supervisory roles and their use of the risk-based approach. Iceland should also explore the specific risks associated with legal persons and arrangements and improve the availability of beneficial ownership information," FACT said.

FAFT said with the exception of the three large commercial banks in Iceland, the financial sector and non-financial businesses and professions have a poor understanding of the money laundering or terrorist financing risks to which they are exposed.

These private sector entities have limited awareness of their AML/CFT obligations and report very few suspicious transactions in light of the risks present, FACT said.

Icelandic authorities cooperate well with counterparts in other countries, particularly their Nordic neighbours, both seeking and providing information on a wide range of cases. "Iceland has a sound legal framework for investigation and prosecution of money laundering. Recently, there has been an upward trend in the number of money laundering prosecutions. Iceland is committed to trace and seize the proceeds of crime, both in Iceland and abroad," FAFT said.

"However, despite the presence of some relevant risk factors, Iceland has not conducted any criminal investigations into terrorist financing, although it has contributed intelligence to investigations initiated by foreign counterparts.

"Iceland must use its ability to coordinate domestic authorities and put practices in place to strengthen its efforts to tackle money laundering and terrorist financing.

"During the assessment, the country demonstrated a commitment to take the necessary action to do so and the FATF welcomes the steps that country has already taken since that time," said FAFT.

Sales manager jailed for laundering HK$3m

A former sales manager of a gift trading company (Company A), has been sentenced to four years' imprisonment at Hong Kong District Court for laundering over HK$3.4 million in crime proceeds in relation to 50 false production orders.

The 46-year-old defendant, was charged by the Independent Commission Against Corruption of Hong Kong (ICAC). The case arose from a corruption complaint. The court heard that at the material time, the defendant was a sales manager of Company A, which was engaged in gift trading business. He was responsible for sourcing gift orders from clients and placing production orders with suppliers.

The defendant submitted 50 production orders to Company A applying for advance payments totalling approximately Renminbi 2.77 million (over HK$3.4 million) payable to two suppliers in the mainland China.

The court heard that in believing the applications were genuine, Company A approved them and remitted the money into the designated accounts of the two suppliers held by two representatives of a licenced remittance agency in Hong Kong.

The representatives of the licenced remittance agency then arranged for the transfer of the corresponding sum of Hong Kong dollars from their bank accounts to the defendant's bank accounts in Hong Kong.

Between November, 2012 and November, 2014, two sums of money, namely over HK$3.1 million and more than HK$310,000, were paid into the defendant's bank accounts in Hong Kong.

Had Company A known that the 50 production orders concerned were false, it would not have approved or endorsed the applications, the court was told.

Bribery and corruption outlook 2018

WHAT is the outlook for bribery and corruption in 2018?

Law firm Hogan & Lovells has published a guide to trends and developments in anti-bribery and corruption.

Below is an extract from its report which can be found at http://bac.hoganlovellsabc.com/_uploads/downloads/12300_D3_Briberyandcorruptionoutlook2018_BRO_E.PDF

FOR the most part, 2018 will see countries do more to enforce their anti-bribery and corruption laws. How authorities plan to go about this — from cooperating with foreign counterparts to adapting others' regimes — differs by jurisdiction. There's no catch-all advice we can give. But we can share our lawyers' insights on areas that might affect you and what to watch out for.

Enforcement

To date, the Trump administration has kept up enforcement of the US Foreign Corrupt Practices Act (FCPA) cases that began under the Obama administration.

The real test, of course, will come when new cases arise. If the result is more of the same, big settlements remain a prospect, too. Seven of the 13 corporate enforcement actions by the US Department of Justice (DOJ) and the US Securities and Exchange Commission (SEC) in 2017 involved non-U.S. companies.

This backs up the Trump administration's promise to counter foreign corruption. And if this continues — there are few signs it won't — individuals and foreign companies beware.

Monitorships

More than half DOJ's 35 deferred prosecution agreements (DPAs) and non-prosecution agreements in 2016 saw companies hire monitors. Six out of 13 settlements with DOJ and the SEC resulted in appointing monitors. These were mostly where the companies' internal controls had failed. Use of monitors is here to stay.

DPAs

Worldwide take up of the DPA regime is some way off, if not unlikely. But as interagency cooperation and cross-border investigations increase, the UK, France, and Italy have become a testing ground.

With prosecutors shaping how they'll work together across jurisdictions, you need to be aware of emerging DPAs in Europe and how it might affect you.

Privilege

Privilege protection varies: documents protected in one jurisdiction may not have the same protection elsewhere. Case law has put privilege in the spotlight in Germany and the UK. We share steps you should know and take.

Bribery redefined

China's new Anti-Unfair Competition Law redefines commercial bribery. It has wider coverage — to include parties with influence over a transaction, for example, though who these are remains unclear — and increased penalties. How it works in practice won't be known until we see judges interpret the law.

Cooperation

International cooperation is up. Authorities and agencies in countries in Africa and Latin America, for example, are working with their foreign counterparts to tackle domestic corruption.

This trend in cooperation goes both ways. The US SEC acknowledged help in FCPA matters from 19 jurisdictions in 2017. Indeed, the larger FCPA resolutions — Telia Company and Rolls-Royce, to name two — were made possible through working with foreign counterparts. Fewer countries now go it alone, in fact, which makes it harder to evade enforcement.

Liability

The criminal liability systems in South East Asia are evolving. As local laws change, authorities collaborate to keep pace, and they do this increasingly well. Enforcement is certain to rise. Seven out of 10 ASEAN jurisdictions have low scores in Transparency International's Corruption Perceptions Index, lower than 100 other jurisdictions.

~ Source: Hogan & Lovells. This guide was first published by Hogan & Lovells.

To find out more, visit www.hoganlovellsabc.com

OECD asks Poland to take urgent steps

POLAND must make urgent progress on carrying out key recommendations of the OECD Working Group on Bribery that remain unimplemented, more than four years after its Phase 3 evaluation in June 2013.

The OECD said Poland still needs to take urgent steps to ensure companies can be held responsible for foreign bribery, even if the persons who perpetrated the offence are not convicted.

"In addition, Poland must increase the fines for companies in order to ensure foreign bribery is punishable by effective, proportionate, and dissuasive sanctions," OECD said. The organisation added, "The Working Group is disappointed by Poland's failure to take measures to ensure that the 'impunity' provision in the Penal Code that applies to foreign and domestic bribery cannot be applied to the bribery of foreign public officials.

"This provision allows perpetrators of bribery to automatically escape

Image: Pixabay

punishment by notifying the law enforcement authorities of the offence before the authorities learn about it from other sources."

In the context of ongoing reforms, OECD said Poland should also ensure that appropriate measures are in place to protect from retaliatory or disciplinary action private and public sector employees who report suspected acts of foreign bribery in good faith and on reasonable grounds.

The Working Group reviewed a report submitted by Poland on its progress in implementing these outstanding recommendations at its plenary meeting in March 2018.

It requested that Poland provide a written report on further progress in addressing these concerns in December 2018, at which time the Group will consider additional measures in the absence of significant progress.

Malaysia to introduce corporate liability for corruption

THE lower house of Malaysia's Parliament has passed a bill that will introduce corporate liability for companies guilty of corruption.

Under the Malaysian Anti-Corruption Commission (Amendment) Bill 2018 an offence committed by a company may be deemed to have been committed by its shareholders, board of directors, or its management. The new bill also broadens liability to include any person who may be a partner or employee of a firm, or who provides services to it, reports *The Edge Markets.*

Reed Smith explains that the definition of commercial organisation has a wide ambit, and includes Malaysian companies and partnerships whether conducting business in Malaysia or outside of Malaysia, as well as foreign companies conducting business in Malaysia. Further, where corporate liability is found, the director, controller, officer (and this would include an employee), partner or "person who is concerned in the management of its affairs" will be deemed to have committed the corrupt offence.

Reed Smith says the onus then shifts to the individual to prove that the offense was committed without their consent, and that they exercised due diligence to prevent the commission of the offense, taking into account the nature of their function in that capacity and the circumstances. "The financial penalties for a commercial organisation that is liable are fairly significant – being the higher of either a monetary fine of not less than 10 times the value of the gratification, or RM1 million," Reed Smith explained.

Reed Smith advises that in the lead-up to its enforcement, companies doing business in Malaysia should prudently begin the process of ensuring that systems are put in place that demonstrate due diligence in preventing corrupt offenses by not only their executives and employees, but also third-party intermediaries such as distributors, vendors and agents.

Transparency International Malaysia president Akhbar Satar said, "We strongly believe that the MACC (Amendment) Bill 2018 will make significant progress in private sector anti-corruption movements.

"As the law will be enforced soon, we also encourage companies to initiate and introduce comprehensive anti-corruption programmes or training in their organisations for their employees and business associates, to mitigate the risk of being held liable by MACC," he said.

Cybercrime

Maritime cyber attacks pose major risks

The maritime industry has been slow to acknowledge the threat posed by cyber attacks but the increasing connectivity of technologies across all layers of the supply chain create a target for hackers. Sarah Gibbons *reports.*

WITH increasing levels of connectivity across global supply chains, the maritime industry faces a significant risk of cyber-attacks.

Training and awareness programmes to combat the threat are gaining momentum to shore up the sector's defences, especially as some insurance policies do not cover shipowners from the damage caused to their businesses.

The potential risks are serious: pirates taking remote control of vessels and diverting them to ports of their choice; international navigation systems being hacked and grounding ships; or paralysing port operations, are some of the more extreme concerns, which have yet to actually happen – thankfully.

But more humdrum risks are maybe of greater importance – crew introducing computer viruses, either maliciously or unwittingly, maybe crippling systems and operations. The true cost of such attacks is unknown because of significant under- or non-reporting by maritime organisations fearing reputational losses.

Cyber awareness

"Crew and the devices they take on board are the source of many of the cyber intrusions that happen at sea," according to a November 2017 report by international law firm Clyde & Co, based in London, and the Institute of Marine Engineering, Science and Technology IMarEST, also based in London, entitled 'Technology in shipping – the impact of technological change on the shipping industry'.)

Yet a survey by IHS Markit's Fairplay maritime publication of shipping industry workers last September revealed that despite 34% of the respondents saying their company had experienced a cyber attack in the previous 12 months, many employees had received little or no cyber awareness training; 30% had no appointed information security manager or department; and a third had no IT security policy. Of the 284 respondents from roles across the industry, 47% believed their organisation's biggest cyber vulnerability was the staff.

This can cut both ways – staff involved in attacks and failing to detect and deal with them, said Mark Milford, vice president cyber security at Wärtsilä, marine solutions experts based in Helsinki, Finland.

"I strongly believe that the education of employees will create an understanding of cyber risk and prove to be a catalyst for change in the technologies and processes used in shipping and the wider industry. A focus on education is therefore paramount."

Report incidents

As many as 80% of cyber issues could have been prevented with better training and awareness, say the Maritime Cyber Alliance, formed last year by Airbus and the CSO Alliance (cyber security officers) to encourage the anonymous reporting of incidents, and which has now launched a Be Cyber Aware At Sea campaign.

Mark Sutcliffe, CSO Alliance managing director, told *Commercial Crime International*: "We need to understand the criminal footprint to be able to calculate risk, and this requires people to report incidents. However…incidents will not be reported unless it is anonymously.

"Many [businesses] simply do not know what to protect and what to invest in and, without insights and a credible threat vector, inertia is ruling."

Vulnerabilities on board ships include outdated and unpatched software, unsegregated networks, lack of access-control to computers and networks, lack of cyber security and safety policies, lack of intrusion detection, obsolete operating systems and low-quality hardware used to construct networks.

Cruise ships are further compromised, potentially, by the sheer volume of passengers onboard on a routine basis, accessing personal devices via ships' systems which, if not isolated, risk being infected with malware.

The sheer number of parties involved in, for example, the shipment of a cargo from A-B, each one's reliance on digitalisation, the rise of the Internet of Things and associated interconnectivity, the multiple jurisdictions involved in registrations and logistics with their varying methods of scrutiny mean there is "an incredibly large attack surface that can be exploited," said Milford.

Weakest link

"Criminals try to get access through the weakest link, so we have to make sure the whole supply chain is resilient," said Aron Soerensen, head of maritime technology and regulation at BIMCO (The Baltic and International Maritime Council), representing shipowners and agents, based in Copenhagen, Denmark.

Onboard systems vulnerable to hackers include cargo management systems; shipment-tracking tools; network navigation systems, with

Continued on page 9/

from page 8 - Maritime cyber attacks

interfaces to shoreside networks; radar; propulsion and machinery management and power control systems; surveillance and shipboard security alarms; boarding and access controls, which may hold valuable passenger related data; guest entertainment systems; administrative and crew welfare systems; engine performance monitoring and maintenance; and spare parts management.

London-based shipbroker Clarkson Plc confirmed a cybersecurity incident which involved unauthorised access to the company's computer systems in November 2017 when confidential data was stolen.

Knock-on effect

In June last year, shipping giant A.P. Moller-Maersk suffered an estimated US$300 million lost revenues when struck by the Petya ransomware attack which brought several global port operations to a halt with associated knock-on disruptions lasting several days. About 4,000 new servers, 45,000 new computers, and 2,500 applications had to be reinstalled as a result.

In 2013, drug traffickers recruited hackers to breach IT systems at the port of Antwerp in Belgium to enable them to work out the location and security details of containers of bananas and timber containing planted illicit narcotics from South America. They sent in drivers to steal the cargo before the containers' legitimate owners arrived. Hackers broke into the docks' offices and fitted special key-logging devices onto computer terminals, allowing them to remotely monitor computer keyboards, and access passwords.

To demonstrate a ship's vulnerability to cyber-attacks, Israel-based cyber defence system producer Naval Dome's engineering team have performed cyber attacks on live navigation systems, engine and other machinery control systems, shifting a vessel's reported position, corrupt the radar display, turn on and disable machinery, and override the fuel control, steering and ballast systems.

A note from the company said in the past decade, cyber attacks against the maritime industry have increased 1,000% and caused damage worth billions of dollars.

Thankfully, guidelines and initiatives being developed to protect assets and systems.

In May (2018), the European Union's (EU) networks and information systems (NIS) directive comes into force, insisting that by September, "operators of essential services" have to be identified, including

Image: Pixabay

transport providers, who must take "appropriate and proportionate security measures to manage risks to their network and information systems, and they will be required to notify serious incidents to the relevant national authority", said the UK's National Cyber Security Centre.

The International Maritime Organisation (IMO) issued its 'Guidelines on Maritime Cyber Risk Management', in July 2017, "to safeguard shipping from current and emerging cyber threats and vulnerabilities". Such measures should be applied alongside existing safety and security management practices "to support safe and secure shipping, which is operationally resilient to cyber risks".

They call on senior management to "embed a culture of cyber risk awareness into all levels of an organisation and ensure a holistic and flexible cyber risk management regime" rather than simply entrusting the issue to IT teams.

Moreover, guidelines on cyber security onboard ships produced and supported by BIMCO, the Cruise Lines International Association (CLIA), International Chamber of Shipping (ICS), INTERCARGO, INTERTANKO, Oil Companies International Marine Forum (OCIMF) and the International Union of Marine Insurance (IUMI) were published last July (2017) and warn: "The safety, environmental and commercial consequences of not being prepared for a cyber incident may be significant". This guidance urges senior management to drive awareness of risks, identify where that lies and it recommends appropriate actions following attacks. Crucially it reminds operators that their insurance policy does not necessarily cover them from cyber damage.

Low-hanging fruit

Lars Lange, secretary general, of IUMI, based in Hamburg, Germany, said: "Cybercrime is not necessarily covered under a typical insurance contract and in some policies, it is not mentioned…"

He believes the proportion of maritime cyber incidents that are reported could be 11% and advised companies "a lot of the threat can be dealt with by going after low hanging fruit – advising about the use of USB sticks, opening email attachments – for all levels of staff".

New cryptocurrency mining methods emerging

2018 and 2019 could see the emergence of a newer technique of mining cryptocurrency which exploits website visitors, the United Kingdom's National Cyber Security Centre (NCSC) has warned.

NCSC's *'The cyber threat to UK business'* 2017-2018 report says that throughout 2017, there was an increase in cryptojacking (using an individual's computer processing power to mine cryptocurrency without their consent).

"In December 2017, Check Point reported that 55 percent of businesses globally were impacted by cryptominers. Popular websites are likely to continue to be targets for compromise, serving cryptomining malware to visitors, and software is available that, when run in a webpage, uses the visiting computer's spare computer processing power to mine the digital currency Monero," the report says.

In February 2018, over 4,000 websites worldwide (including approximately 600 in the UK) secretly mined cryptocurrency through a compromised screen-reading plugin for blind and partially sighted people. The only way users may notice their devices are being cryptojacked is a slight slowdown in performance.

Using an ad blocker or antivirus programme (which have features that block browser mining) is the best way to prevent this, NCSC says.

"We assume the majority of cryptojacking is carried out by cyber criminals, but website owners have also targeted visitors to their website and used the processing power of visitors' CPUs, without their knowledge or consent, to mine cryptocurrency for their own financial gain, the report said.

"In February 2018, a US online publication conducted a trial where its readers were advised that if they chose to block its advertising, the publication would use the reader's CPU to mine Monero. It claimed this was to recoup lost advertising revenue when readers use ad blockers."

Business Email Compromise (BEC)

NCSC said the growth of BEC is unlikely to result from significant technological developments; rather criminals are continually honing techniques to exploit victims.

1. Payments fraud surge

78% of organisations were still impacted in 2017.

2. Cheques still main target of fraudsters

A staggering 75% of finance professionals report that their organisations' cheque payments were exposed to fraud.

3. Business email compromise still popular

77% of organisations experienced fraud via Business Email Compromise in 2017. From CEOs to treasury analysts, anyone and everyone is a likely target.

* *Source: Association for Financial Professionals – Payments Fraud and Control Survey Report*

They use increasingly sophisticated techniques that often include a combination of social engineering, email phishing, email spoofing and malware. There has been a noticeable change in trends, moving from exploit kits to social engineering emails with malicious attachments. This is largely due to systems being upgraded and patched, so exploit kits no longer work as well as they used to.

"BEC scams are a serious threat to organisations of all sizes and across all sectors, including non-profit organisations and government. It represents one of the fastest growing, lowest cost, highest return cybercrime operations," the report says.

Industry experts project that global losses from BEC scams will exceed US$9 billion in 2018.

In 2017, Dublin Zoo was hit by a BEC scam, with cyber criminals reportedly obtaining nearly US$ 600,000. They allegedly intercepted legitimate supplier invoices sent to the zoo and manipulated data on the documents to change payment details and account numbers, requesting that funds be sent into a fraudulent account.

Other examples highlight a string of BEC attacks on the art industry, when art galleries and dealers have been targeted by invoice scams after cyber attackers infiltrated their emails.

Financial sector compromise
Mitigations against financial sector compromise. The NCSC recommends that businesses:

- use up-to-date and supported operating systems and software
- deploy critical security patches as soon as possible
- deploy an always-on antivirus solution that scans new files
- conduct regular vulnerability scans and action critical results
- implement application whitelisting technologies to prevent malware running on hosts
- implement a policy of least privilege for all devices and services
- establish configuration control and management

Cybercrime costs businesses close to $600bn

CYBERCRIME costs businesses close to $600 billion, or 0.8 percent of global GDP, according to a report, up from a 2014 study that put global losses at about $445 billion.

The report attributes the growth over three years to cybercriminals quickly adopting new technologies, the ease of engaging in cybercrime – including an expanding number of cybercrime centres – and the growing financial sophistication of top-tier cybercriminals. The report – '*Economic Impact of Cybercrime – No Slowing Down'* - was carried out by McAfee, in partnership with the Center for Strategic and International Studies (CSIS).

"The digital world has transformed almost every aspect of our lives, including risk and crime, so that crime is more efficient, less risky, more profitable and has never been easier to execute," said Steve Grobman, Chief Technology Officer for McAfee.
"Consider the use of ransomware, where criminals can outsource much of their work to skilled contractors. Ransomware-as-a-service cloud providers efficiently scale attacks to target millions of systems, and attacks are automated to require minimal human involvement.

"Add to these factors cryptocurrencies that ease rapid monetisation, while minimising the risk of arrest, and you must sadly conclude that the $600 billion cybercrime figure reflects the extent to which our technological accomplishments have transformed the criminal economy as dramatically as they have every other portion of our economy," he added.

Banks remain the favourite target of cybercriminals, and nation states are the most dangerous source of cybercrime, the report finds. Russia, North Korea and Iran are the most active in hacking financial institutions, while China is the most active in cyber espionage.

"Our research bore out the fact that Russia is the leader in cybercrime, reflecting the skill of its hacker community and its disdain for western law enforcement," said James Lewis, senior vice president at CSIS.
"North Korea is second in line, as the nation uses cryptocurrency theft to help fund its regime, and we're now seeing an expanding number of cybercrime centres, including not only North Korea but also Brazil, India and Vietnam."

The report measures cybercrime in North America, Europe and Central Asia, East Asia and the Pacific, South Asia, Latin America and the Caribbean, Sub-Saharan Africa, and the Middle East and North Africa. Not surprisingly, cybercrime losses are greater in richer countries. However, the countries with the greatest losses (as a percentage of national income) are mid-tier nations that are digitised but not yet fully capable in cybersecurity.

The report did not attempt to measure the cost of all malicious activity on the internet, focusing instead on criminals gaining illicit access to a victim's computer or network. The elements of cybercrime the authors identify include:

- The loss of IP and business-confidential information.
- Online fraud and financial crimes, often the result of stolen personally identifiable information.
- Financial manipulation directed toward publicly-traded companies.
- Opportunity costs, including disruption in production or services and reduced trust in online activities.
- The cost of securing networks, purchasing cyber insurance and paying for recovery from cyber-attacks
- Reputational damage and liability risk for the affected company and its brand.

Recommendations

The report also includes some recommendations on how to deal with cybercrime, including:

- Uniform implementation of basic security measures and investment in defensive technologies.
- Increased cooperation among international law enforcement agencies.
- Improved collection of data by national authorities.
- Greater standardization and coordination of cybersecurity requirements.
- Progress on the Budapest Convention, a formal treaty on cybercrime.
- International pressure on state sanctuaries for cybercrime.

HIGHLIGHTS

- Theft of intellectual property accounts for at least 25 percent of cost of cybercrime .
- Ransomware is the fastest growing cybercrime tool, with more than 6,000 online criminal marketplaces and ransomware-as-a-service gaining in popularity.
- Cybercrime-as-a-service has become more sophisticated, with flourishing markets offering a broad diversity of tools and services such as exploit kits, custom malware and botnet rentals.
- The anonymity of cryptocurrencies such as Tor and Bitcoin protects actors from easy identification.
- Greater standardisation of threat data and better coordination of cybersecurity requirements would improve security, particularly in key sectors like finance.
  *The report can be found here.

Cybercrime

Shipowners urged to be cautious over Petros transactions

FOREIGN shipowners trading with Venezuela have been advised to exercise caution to be certain that any remittances made through the United States' financial system in connection with their Venezuelan trade are not ultimately being used to purchase the Venezuelan cryptocurrency Petros.

US maritime law firm, Freehill, Hogan & Mahar has issued a client alert in which it anticipates that US banks will scrutinise all financial transactions relating to Venezuela with great care, particularly those involving shipping, in the wake of a recent directive and a circular.

On March 19 President Trump issued Executive Order 13827, which prohibits US persons and persons within the US from providing financing for or engaging in any dealings in "any digital currency, digital coin or digital token" issued by Venezuela on or after January 9, 2018, which includes the Petro.

On March 23rd the National Institute of Aquatic Spaces (INEA), which acts as the Venezuelan maritime authority, issued a Circular to all shipping agencies in Venezuela, advising that payment for all services rendered to foreign flag vessels must thereafter be paid in Petros.

"This means that foreign shipowners will have to pay for such services as pilotage and towage in Petros. Reportedly, there is a possibility that the requirement for Petros payments may be extended to other maritime services provided by government agencies in Venezuela," Freehill, Hogan & Mahar said.

It cautioned that the requirement that payment for shipping services provided by Venezuelan governmental agencies be made in Petros may expose foreign shipowners to the prohibitions of E.O. 13827.

In addition to preventing US persons from engaging in any transactions relating to Venezuelan digital currency, E. O. 13827, in Section 2, prohibits any transaction "… that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in this order…."

Freehill, Hogan & Mahar said, "It is our understanding that foreign shipowners often remit funds on account to Venezuelan ship agents in order to pay port charges and vessel disbursements. Such remittances are often made in US dollars and move through the US banking system.

"Since it now appears that a portion of such advances paid by foreign shipowners may be used by local Venezuelan shipping agents to purchase Petros, in order to make the required payments in that digital currency, US banks would be engaged in a transaction "related to" Petros.

"Informal discussions with the US Office of Foreign Asset Control indicate that a bank which processes an advance payment to a Venezuelan port agent, a portion of which would used to purchase Petros, would be in violation of E. O. 13827.

"Furthermore, the foreign vessel owner who instructs the bank to make such a remittance, knowing that a portion of the remittance would be used in dealing in Petros, would also be in violation of E. O. 13827, because it would have caused a violation of the E. O. by a US bank," Freehill, Hogan & Mahar said.

In January this year, President Maduro of Venezuela announced that Venezuela would issue its own cryptocurrency, Petro, which would be backed by the country's petroleum reserves.

The move was designed to minimise the impact of the US prohibition on the extension of new debt and to create a new means of payments for goods and services.

* *Source: Freehill, Hogan & Mahar*

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