Commercial Crime International

August 2023

ICC Commercial Crime Services
A specialised division of the International Chamber of Commerce

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

Helping Business Stay in Business since 1981

IMB raises concern over piracy resurgence in Gulf of Guinea

SIXTY-FIVE incidents of piracy and armed robbery against ships were reported to the International Maritime Bureau Piracy Reporting Centre (IMB PRC) in the first half of 2023 compared to 58 in the same period last year.

Of the 65, a total of 57 vessels were boarded. There were four attempted attacks, two hijackings and two vessels fired-upon.

More disturbingly, perpetrators successfully boarded 90 percent of the ships targeted globally, and violence towards crews continues to be a worry, with 36 crew taken hostage, 14 kidnapped, three threatened, two injured and one assaulted.

Rising concerns in Gulf of Guinea

The Gulf of Guinea witnessed a concerning surge in maritime incidents between Q1 and Q2 of 2023, with five incidents in the first quarter and nine in the second quarter.

Fourteen crew were kidnapped in the region, eight of whom were taken from ships anchored within territorial waters in two separate incidents. Additionally, 31 crew were taken hostage in two separate hijackings and the ships' communication and navigation equipment destroyed with some cargoes stolen. Six crew were also kidnapped in one of these incidents.

Upon receiving these reports, IMB PRC was able to swiftly help coordinate the necessary response to assist the ships and crew. IMB commends and thanks the French authorities and the naval asset which assisted to locate both these hijacked vessels.

Nevertheless, IMB is warning that it is by no means 'game over'. IMB Director Michael Howlett said, "The resurgence in reported incidents including hostage situations and crew kidnappings in the Gulf of Guinea waters is concerning. The IMB calls for continued, robust regional and international naval presence as a deterrent to address these crimes."

Bigger ships targeted in Singapore Straits

Vessels transiting the Singapore Straits continue to be targeted and boarded, and there has been a 25 percent increase in reported incidents compared to last year, in these busy and congested waters.

The perpetrators successfully boarded all 20 ships, 19 of which were underway. While considered low level opportunistic crimes, IMB notes that crew continue to be at least eight of those incidents.

Large bulk carriers account for 13 of the incidents, with the rest being tankers and low and slow tugs and barges. This appears to be an upscaling of attacks, where previously pirates targeted mostly smaller and slower vessels.

Though considered as low level opportunistic thefts, IMB requests littoral states to allocate the required resources to address these crimes as crew members continue to be at risk. Moreover, these incidents could present a major risk, potentially resulting in the loss of ship, cargoes and crew, because they are taking place in one of the world's busiest and congested sea routes.

Indonesian archipelagic region

The Indonesian archipelagic region has shown a sustained decrease in reported incidents compared to years preceding 2020, with seven incidents reported, primarily involving anchored or berthed vessels. Crew members remain at risk, with instances of threats and knives reported.

South and Central America

In South and Central American ports, which accounted for 14 percent of global incidents, there were 13 reported incidents, including attempted boardings, hostage situations, crew assaults and threats

Continued on page 2/

In This Issue of CCI

Top UN official in Africa calls for more action

INTERNATIONAL cooperation is making waves in combatting piracy in West Africa, but addressing its root causes and ensuring sustainable funding must fully eliminate threat, which is spreading to other regions, a top UN official has told the Security Council.

Despite gains made in tackling sea-faring criminal groups, "piracy incidents continue to threaten the safety of maritime traffic in the region," said Martha Pobee, UN Assistant Secretary-General for Africa in the Departments of Political and Peacebuilding Affairs and Peace Operations.

Since her last briefing on maritime security in November, she said a steady decrease in piracy incidents in the Gulf of Guinea was in large part due to interventions by national authorities and regional and international partners.

Together, these effective deterrents against criminal groups have been buttressed by the ongoing operationalisation of the so-called Yaoundé architecture, established in 2013 with the signing of the related Code of Conduct by actors in the region, she said, noting that four out of five interregional coordination centres are now functioning.

Such efforts, including forming joint naval task groups, have enhanced cooperation and information sharing while forging a centralised process for maritime security that bridges national and regional capacity gaps, she said.

Threats shifting waters

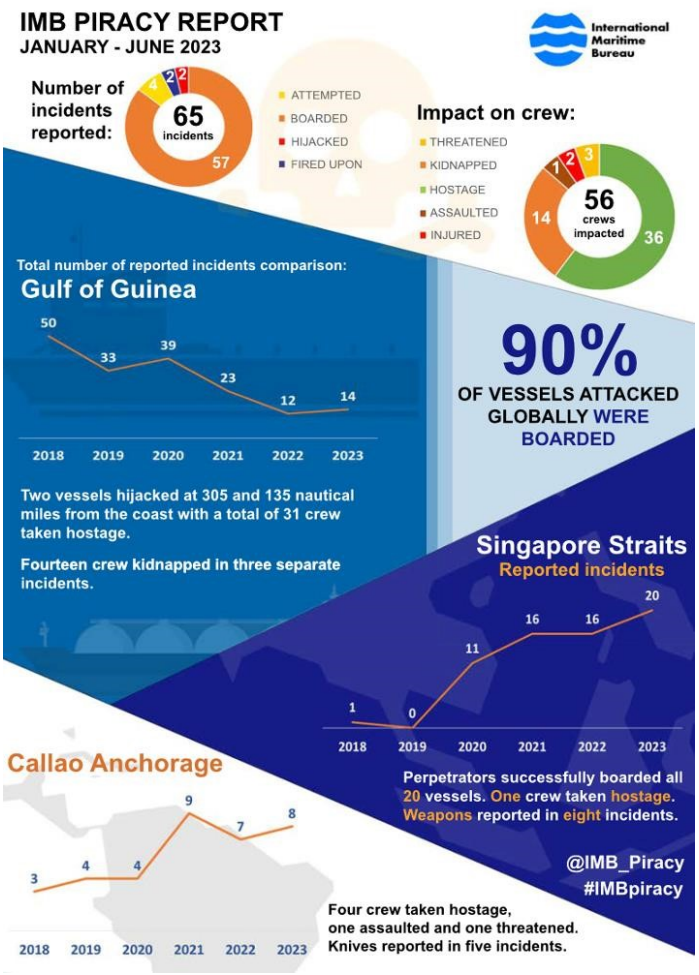
However, gaps remain, she cautioned, calling for increased support to fill them. These include such challenges as the lack of appropriate equipment and of sustainable financing to ensure the full operationalisation of the Code of Conduct.

Recent figures already suggest that "incidents are steadily shifting from the waters of West Africa towards the maritime domain of the UN Economic Community of Central African States, she said.

Key action areas

Underlining several key areas essential for success in reviewing the Code, she said nations must first update legal frameworks. Meanwhile, enhanced coordination between the Interregional Centre and partners "remains vital".

In addition, actors must address the root causes of piracy to eliminate the threat, she said.



from page 1- reporting vital

at Callao Anchorage in Peru, Colombia, Macapa Anchorage in Brazil, and Panama.

Vital point of contact

IMB remains resolute in its role to ensure the crime of piracy and armed robbery against ships is kept high on the agenda of governments and the international shipping community, with any escalation having a direct impact on the safety of seafarers and the vital trade they carry. Whilst it is vital for robust action to be taken against these criminals, it is equally important that there is timely reporting of incidents to the IMB PRC.

Founded at a time when seafarers had little option to report incidents, IMB PRC remains a single point of contact to report all crimes of maritime piracy and armed robbery, 24 hours a day.

Since 1991, the Centre's prompt forwarding of reports, and liaison with response agencies, broadcasts to shipping via GMDSS Safety Net Services, and email alerts, all provided free of cost, help the response against piracy and armed robbery globally. As evidenced by the standing up of multiple regional cooperation, reporting and response mechanisms, its reports have over time increased awareness, resulting in the allocation of adequate resources to make waters safer.

Australia targets investment scams

AUSTRALIA'S National Anti-Scam Centre will coordinate an investment scam fusion cell to combat the growing problem of investment scams, which are costing the country's citizens more than $1 billion a year.

The fusion cell will be led by the Australian Competition and Consumer Commission (ACCC) and Australian Securities and Investment Commission (ASIC) and include representatives from the banks, telecommunications industry and digital platforms.

It will be the first fusion cell co-ordinated by the new National Anti-Scam Centre and will identify methods for disrupting investment scams to minimise scam losses.

Fusion cells are time-limited taskforces designed to bring together expertise from government and the private sector to take timely action to address specific, urgent problems.

The National Anti-Scam Centre will coordinate a series of fusion cells with different participants to target particular scam types.

"Investment scams lead to the highest level of reported individual losses and cause emotional devastation for victims," ACCC Deputy Chair Catriona Lowe says.

"That is why the National Anti-Scam Centre is prioritising investment scam disruption as its first fusion cell in an initiative that facilitates timely action by finance, telecommunications and digital platforms to stop scammers."

"This additional level of co-ordination and focus across government and relevant industries will target investment scam activity more effectively and help prevent further losses to these scams," Ms Lowe added.

ASIC Deputy Chair Sarah Court welcomed the announcement of the fusion cell and said ASIC looked forward to sharing its expertise in investment scams with the National Anti-Scam Centre.

ASIC and the ACCC working together as part of the National Anti-Scam Centre's first fusion cell is an important step towards protecting Australians from harmful investment scams," Ms Court said.

"A collaborative approach that sees regulators working with each other, as well as with the private sector, is crucial to addressing this challenge," she concluded.

Investment scam fusion cell aims

The investment scam fusion cell will be set up initially for six months, with the National Anti-Scam Centre publicly reporting outcomes. The fusion cell will aim for:

- Early intervention to disrupt investment scams including stopping scammers from reaching potential victims.
- Removing investment scam websites from the internet.
- Sharing information about investment scam activity to assist the private sector to take disruption action
- Providing information to the public so they can avoid investment scams identifying intelligence to refer to law enforcement in Australia and overseas.

New Singapore registry to curb trade finance fraud

The Association of Banks in Singapore (ABS) has launched an industry utility that will securely maintain a centralised record of trade finance transactions in Singapore.

The Trade Finance Registry (TFR) is supported by key trade financing banks in Singapore.

This industry initiative aims to mitigate the risk of duplicate financing for the same underlying trade and will enhance trust and confidence among banks and traders, and strengthen Singapore's role as a key trading hub.

TFR will remove the information asymmetry faced by banks and facilitate the detection of duplicate financing.

Participating banks will register new trade financing transactions on TFR, and if any of the new transactions are found to be duplicated, this will trigger notifications in near real-time for further action.

Only information on corporate customers will be provided to the TFR. In addition, data on the TFR is hashed into an encrypted format.

As such, matching of duplicate trades can be done without exposing the banks' underlying data fields to other participating banks.

TFR will also improve the transparency of trade financing transactions by enhancing their ability to validate authenticity of trade, through API connections to the Singapore Trade Data Exchange (SGTraDex), a public digital platform that facilitates trusted and secure sharing of data between supply chain ecosystem partners.

Money Laundering

EU action plan: will it reduce cross-border financial crime?

ICC FraudNet has launched the third edition of its Global Annual Report which takes as its theme "Fraud and Asset Recovery in an Unstable World". The 2023 Report comprises 28 original articles authored by 52 contributors, from some 20 jurisdictions who make up FraudNet's unparalleled global network of leading fraud and asset recovery lawyers, strategic partners, and associated collaborators from the investigative, consulting, advisory and academic worlds. Over the next few months, CCI will be highlighting extracts from some of the articles. The first is authored by FraundNet members Diane Bugeja, Senior Associate, and Peter Mizzi, Compliance and AML Advisor at Camilleri Preziosi Advocates.

Introduction

On 20 July 2021, the European Commission (the 'Commission') formally announced its proposal (the 'Proposal') for a regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of Money Laundering or Terrorist Financing ('ML/FT'). The proposal consists of an aspiring package that seeks to overhaul the current 1COM/2021/420 final 86 European Union ('EU') Anti-Money Laundering and Countering the Financing of Terrorism ('AML/CFT') regime, focusing on the consolidation and harmonisation in an attempt to overcome existing gaps and loopholes in the current framework, most prominently at the cross-border level. Given the cross-border nature of financial crime, it is critical that member states (MS), national supervisors, and Financial Intelligence Units ('FIUs') cooperate and coordinate with each other in sharing and dissemination of intelligence.

A regulation establishing an EU AML/CFT authority (in the form of a decentralised EU regulatory agency)

The proposal for a Regulation creating the Anti-money laundering authority ('AMLA') establishes an integrated, EU-level supervisor for combatting ML/FT whilst also acting as a support and cooperation framework for FIUs (which takes the form of a Directive as seen below). Following the successful implementation of the EU AML single rulebook, the AMLA will be at the heart of a revamped EU AML/CFT supervisory system, directly supervising the highest-risk financial institutions that operate in a large number of MS.

Through the AMLA's coordination of national supervisors, it will indirectly supervise the remaining financial and non-financial entities that fall under the EU AML/CFT framework. The AMLA will possess the power to act on its own behalf if it is found that the local supervisory regime is not enforcing EU law. Therefore, it is anticipated that regulatory emphasis will shift toward those MS where local regulators have been traditionally less active or effective. Further where an entity, not directly supervised, is exposed to very substantial ML/TF risk, then financial supervisors need to provide formal notification to the AMLA.

A new regulation on AML/CFT, containing directly applicable rules, include revised EU list of entities subject to AML/CFT rules (known as Obliged Entities)

Going forward AML/CFT rules applicable to obliged entities will take the form of regulation as opposed to a directive.

Increased scope of obliged entities:

Crypto-Asset Service Provides ("CASPs"), unregulated crowdfunding platforms, creditors for mortgage and consumer credits and associated intermediaries as well as investment migration operators are now considered obliged entities and thus subject to the AML/CFT framework.

Internal Policies, controls and procedures:

Building on existing EU AML/CFT legislation, the new requirements provide clarity on how obliged entities are to identify, analyse, mitigate and monitor ML/FT risks through the implementation of AML/CFT policies, controls and procedures.

Customer due diligence measures:

Most of the existing Customer Due Diligence ('CDD') requirements will take the form of regulatory technical standards provided by the AMLA and will be transferred from the current AML/CFT rules.

Beneficial Ownership:

Building on existing EU AML/CFT legislation, the proposals for updated beneficial ownership rules will streamline the process of transparency among MS.

A proposal for a Directive establishing the mechanisms that Member States should put in place to prevent the use of the financial system for ML/FT purposes, and repealing Directive (EU) 2015/849

The Regulation creating the AMLA and its accompanying Directive provide a support and collaboration system for FIUs, whereby the AMLA will ensure consistent reporting, assist FIUs with a comparative analysis of STRs and also host the FIU.net platform.

Conclusion

The Commission's plan is extensive, ambitious and seeks to completely overhaul the existing AML/CFT legislative framework in a manner that is substantial when compared

Continued on page 5/

from page 4 - harmonised approach potentially useful

to its predecessors. The proposals acknowledge that the cross-border nature of ML/FT requires a coherent and consistent approach across MS, based on a single set of rules in the form of a single rulebook.

Seeing as the present proposal does not adopt a maximum harmonisation approach, several cross-border loopholes were present throughout the Union, exposing the financial system to risks. Shifting the form of AML/CFT rules to a Regulation, with more detail than at present in the EU Directive, will promote convergence of application of AML/CFT measures across MS.

Such will be based upon a consistent framework against which AMLA will be able to monitor the application of such rules in its function as a direct supervisor of certain obliged entities. This being said, the application of a risk-based approach remains fundamental to the nature of the EU's AML/CFT regime.

In areas where specific national risks justify it, MS remain free to introduce rules going beyond those laid out in the present proposal. It can be argued that the notion of the risk-based approach may defeat the purpose of having a set of harmonised rules, however, it is anticipated that the application of a risk-based approach will be closely monitored by national supervisors and the AMLA. The plan to establish a separate, well-resourced EU supervisor promises to increase consistency, uniformity, standards, and degree of AML/CFT supervision across the bloc.

AMLA will work toward ensuring that national supervisors apply the single rulebook in a consistent manner. Nonetheless, obliged entities and FIU may encounter potential compliance challenges such as a lack of cooperation among competent authorities, both at a domestic and cross-border level, creating loopholes that can be misused by criminals.

Additionally, these proposals may come into conflict with other key pieces of legislation namely data privacy acts. Obliged entities will be faced with the improbable challenge of complying with conflicting regulations, whereas AML/CFT requires the processing of personal data, data protection regulations restrict such.

In conclusion, providing a harmonised approach to key areas such as the CDD process, identification of beneficial ownership, reporting procedures as well providing clearer rules for AML/CFT risk management, improving cooperation among authorities, the interconnectivity of bank account registers, the traceability of crypto-assets and increased scope of obliged entities, superseded by consistent application by competent authorities and regulators is highly likely to reduce the cross-border element of financial crime.

The final texts of the legislative proposals are subject to change and refinement, as other EU bodies and stakeholders provide feedback. Therefore, MS, national regulators and obliged entities are strongly encouraged to closely monitor the developments in this space.

* The full article can be found in the Report here.

IMB Internet Intelligence Course

MEMBERS are reminded that International Maritime Bureau (IMB) is holding its popular and useful Internet Intelligence Course: How to Find, Manage and Use Online Information More Effectively from 9th to 12th September.

This comprehensive training course will teach members how to conduct more effective online investigations and find, better information online in less time, at less cost, with less risk. The internet can provide a wealth of information, generating relevant, timely and actionable intelligence, assessing and managing risk, maximising opportunities, assuring compliance, and managing reputation; however, the trick is knowing where to look and how to get there, which is what the well-structed training program aims to do. From routine investigations conducted by frontline personnel to global, tactical and strategic Open Source Intelligence (OSINT) operations, Online and Social Media Research and Investigation skills are essential requirements at all levels of an organisation.

The course is aimed at managers, front-line investigators, researchers and analysts alike, and will be conducted by OSNIT experts Toddington International Inc, who will provide detailed instruction in effectively using the Internet as an Open Source Investigation and Research Tool. This course will also introduce a number of case studies that highlight and correct some errors that have compromised investigations in the past.

Among the valuable learnings and tips for the picking include advanced search engine techniques, the "deep web" - public directories and databases, locating and linking people, places and things, using rss feeds and news aggregators, evaluation and analysis of internet sourced data, strategies and tactics for developing a research plan, and investigating blogs, wikis and social networking sites.

For more details and to register go to IMB's website here.

Experts seek dedicated group to develop common approach

THE first-ever major meeting of high-level experts on Money Laundering and Asset Recovery was organised by Eurojust at its premises in The Hague on 19 and 20 June.

The aim of the meeting was to gather the broadest group of specialists to develop a common approach to take on the increasing crime of money laundering and to improve asset recovery.

The meeting brought together dedicated prosecutors specialised in asset recovery and tackling money laundering from the European Union and countries with liaison prosecutors at Eurojust.

Representatives of the European Commission, other EU Agencies and bodies, the Financial Action Task Force, the CARIN Network, Interpol and other law enforcement agencies participated. Experts in cryptocurrencies, as well as representatives of Financial Intelligence Units and the Egmont Group, joined the meeting.

Experts shared lessons learnt from money-laundering investigations and prosecutions and discussed the various legal challenges and best practices regarding the recovery of criminal assets, notably in view of the Regulation on Mutual Recognition of Freezing and Confiscation Orders and the Trade and Cooperation Agreement between the EU and the UK.

Discussions were timely in the context of the current European Commission proposals in the field of Money Laundering, Asset Recovery and violation of Union restrictive measures.

Special attention was paid to the dimension of cryptocurrencies in the field of asset recovery and money laundering. Participants underlined the importance to have common approaches and to exchange experiences regularly.

In view of this, participants expressed strong support to set up a dedicated Focus Group on Money Laundering and Asset Recovery organised by Eurojust. The aim of this group would be to increase national and cross-border inter-institutional cooperation between the judiciary, law enforcement and other actors involved in the fight against money laundering and the recovery of criminally gained assets, in order to increase efficiency.

In the margins of the meeting, United States Attorney General Merrick B. Garland expressed his support for the shared goal of the European Union and the United States to fight organised crime by countering money laundering and recovering the proceeds of crime.

Money laundering is one of the top three crime types for which national authorities ask for cross-border judicial cooperation via Eurojust.

Last year, the Agency handled a total of 1,882 cases regarding money laundering, of which 690 were opened in 2022.

FATF urges vigilance as Russian aggression continues

FINANCIAL institutions in the United States are being asked to be vigilant to current and emerging risks from the circumvention of measures taken against the Russian Federation in order to protect the international financial system.

A public statement by the Financial Action Task Force (FATF), notes that the Russia's war of aggression against Ukraine continues to run counter to FATF's principles and thus the suspension of the membership of the Russian Federation continues to stand.

The FATF also updated its lists of jurisdictions with strategic anti-money laundering, countering the financing of terrorism, and countering the financing of proliferation of weapons of mass destruction (AML/CFT/CPF) deficiencies. It said U.S. financial institutions should consider the FATF's stance toward these jurisdictions when reviewing their obligations and risk-based policies, procedures, and practices.

The FATF's list of High-Risk Jurisdictions Subject to a Call for Action remains the same, with Iran and the Democratic People's Republic of Korea (DPRK) still subject to FATF's countermeasures. Burma remains on the list of High-Risk Jurisdictions Subject to a Call for Action and is still subject to enhanced due diligence, not counter measures. As part of the FATF's listing and monitoring process to ensure compliance with its international standards, the FATF issued two statements.

The first is the Jurisdictions under Increased Monitoring, which publicly identifies jurisdictions with strategic deficiencies in their AML/CFT/CPF regimes that have committed to, or are actively working with, the FATF to address those deficiencies in accordance with an agreed upon timeline.

The second is the High-Risk Jurisdictions Subject to a Call for Action, which publicly identifies jurisdictions with significant strategic deficiencies in their AML/CFT/CPF regimes and calls on all FATF members to apply enhanced due diligence, and, in the most serious cases, apply counter-measures to protect the international financial system from the money laundering, terrorist financing, and proliferation financing risks emanating from the identified countries.

ML and fraud trends pose diverse threats to companies

Increasingly sophisticated fraud and money laundering are growing concerns, with the need to innovate to tackle diverse threats being underlined at the Association of Certified Fraud Examiners (ACFE) global conference **Keith Nuthall** and **Andreia Nogueira** report.

SPEAKING at the June 12-15 conference's keynote session, ACFE CEO Bruce Dorris said commercial crime specialists needed to continue honing their skills as risks develop: "We must rise; we must inspire; we must innovate. These past few years have been anything but smooth sailing. Organisations around the world were challenged by period of new and unforeseen obstacles including the abundance of opportunities afforded to fraudsters…"

The fraud and money laundering fallout of the Covid-19 pandemic continues, with one speaker Dwayne King, a Canadian senior manager at accounting network Grant Thornton, and a former Toronto police officer, explaining how an Ontario government official had bilked Canadian dollars CA$11 million from an education grant programme.

It was designed to get CA$250 out to all Ontario schoolchildren, so their parents could afford decent internet connectivity and laptops to access online learning during the pandemic.

But the official in charge of the programme brazenly routed 44,000 payments to 250 different bank accounts, mostly in the names of himself, his wife and son. The names of the payees did not have to match the bank account names under lax Ontario government fraud controls.

Once being detected - following bank warnings made to the Ontario government - Sanjay Madan subsequently admitted in court to a past lucrative kick-back scheme fleecing would-be government contractors – which meant he had defrauded the provincial government CA$47 million in total. He was sentenced to 10 years' jail in April (2023).

Fintech fraud

One new trend gaining significant attention at the conference was the rise in fraud risk posted by the expansion of the fintech sector, expanding fast at the expense of traditional banking.

Steve Lenderman, SVP fraud prevention and investigations for digital banking platform BM Technologies, said with 11,000 fintechs in the USA, it was a large and probably unsustainable sector, and one that had significant fraud exposure.

By contrast to established banks, fintechs have smaller staffs, especially regarding anti-fraud, and an over-reliance on tech to screen out bad actors: "Lots of data; lots of tech; minus controls - equals fraud," he commented, noting that fintechs sometimes under-invested on fraud compliance, at a significant risk: "Fintechs must embrace fraud protection. If they don't, they're toast," he said.

A key problem is that to satisfy investors, fintechs need lots of accounts, often of low value – encouraging them to ignore red flags that accounts could be fraudulent or created to move dirty money. Many tech specialists running fintechs think remote know-your-customer (KYC) systems are sufficient to weed out the bad actors, but Lenderman stressed that this was not the case.

Anti-fraud specialists need to work closely with tech developers, he stressed, to educate often unworldly IT experts into human dishonesty. For instance, most fintech customers want to be (and are) onboarded in minutes, these mainly Generation Z and Millennial consumers have no patience for slow systems.

But fraudsters will take their time – if they spend five minutes or more, BM Technologies systems asks additional questions, and if a tardy applicant gives up and comes back for a second try – the system rejects their application – they are likely to be dishonest.

Basic precautions

Another issue is that fintechs often use third party companies to run call centres – who want to get callers off the phone ASAP and refer them back to online services – Lenderman said fintechs need to be live to that risk – phone services need also to detect fraudsters. But conference speaker Ashley Skaale, director and head of fraud operations at the Oregon, US-based First Tech Federal Credit Union told the conference that financial services and fintech really should take more care to avoid losses to fraud.

Part of that is taking basic steps, such as advising clients not to share online banking usernames as well as their passwords, and make sure these are long and complex, to avoid detection through "big server rooms" that criminals use to guess passwords through software matching against standard words.

She says fintechs need to advise their clients against clicking on links in emails, even if they are from someone familiar: "E-mail is one of the worst secure places. It is so not secure. just consider that everything in your e-mail is probably being read by someone. And don't ever click the links..."

Continued on page 8/

from page 7 - uniting AML and anti-fraud teams

Skaale recommends financial institutions, for instance, consult the USA Federal Reserve's FraudClassifier model to better understand fraud involving payments, invest in cross-training and cooperation among departments and having a "fraud governance structure". Skaale also advised companies invest in early warning systems, behavioural biometrics, and report client loss fraud losses to law enforcement.

Ransomware defence

Anthony Hendricks, founder and chair of the Cybersecurity and Data Privacy Practice Group at the Oklahoma, US-based law firm Crowe & Dunlevy, recommended that companies still take precautions to defend themselves against ransomware attacks – which remain expensive – costing US schools and colleges alone US$3.5 billion in 2021.

He highlighted the value of the USA Department of Justice (DOJ) Civil Cyber-Fraud Initiative to "address cyber risk and fraud from companies contracting with the government", he stressed.

The initiative involves companies failing to adequately protect themselves against cyber attacks who cover up such breaches when they happen, to be liable to civil legal action. It "allows the government to collect up to treble damages" of the amount lost to fraud and "allows private citizens to … file actions on behalf of the government", who "are actually able to get a percentage of the money that is recovered", he noted.

As a result, Hendricks advised companies to first understand all their cyber requirements and their risks, depending on their activities, and request assistance if needed. Furthermore, he added, companies should develop "a strong breach response plan", train different teams and leaders, and implement "strong internal programmes to address employee complaints when it comes to criticism about cybersecurity" because "most employees don't want to be a whistleblower" but when their manager fail to listen, they eventually decide to cooperate with the government.

Merging anti-fraud and AML teams

One way of efficiently managing such anti-crime actions, said another speaker, is utilising the developing trend of uniting anti-fraud and anti-money laundering (AML) teams at banks, money service businesses, insurers and other financial institutions.

Called FrAML, this involves close organisational linkages, or even the integration of anti-fraud with AML teams. Ryan Schwoebel, director, special investigative unit, Protective Life Corporation, a US-based life insurer, said FrAML can help fraud investigators spot ML and AML teams identify frauds, which might otherwise be missed. He highlighted the Bernie Madoff case, where JP Morgan Chase had to pay out US$2.6 billion regarding its failures to detect his swindle.

AML officers can develop "tunnel vision" he warned: "When you're focusing only on looking for AML you miss a significant fraud like Ponzi scheme activity… The fraud expert might recognise the fraud activity but…not the movement of funds as consistent with money laundering."

In his experience, FrAML can also boost compliance assessments of companies by financial regulators. FrAML is particularly well suited to mid-sized banks, who may train anti-fraud and ML officers in both disciplines and create integrated reporting structures, he said, although larger international banks may struggle to link the two anti-crime units because of conflicting multi-country regulatory issues, he warned.

In any case, the conference host the ACFE is certainly well-placed to train and inform anti-fraud and anti-money laundering professionals fighting such commercial crime.

ACFE VP membership Ross Pry told the conference that it currently has 92,000 members in more than190 countries around the world, of whom 62,000 are certified fraud examiners (CFEs) with the remainder being internal auditors, accountants, risk managers, law enforcement agents, compliance and ethics professionals and other specialists: "These disciplines come together and they work with each other to share a common goal to detect and fight fraud," said Mr Pry.

THE Extractive Industries Transparency Initiative (EITI) has launched the 2023 EITI Standard, the fourth edition of the global standard for transparency and good governance of the oil, gas and mining sector. The amended EITI Standard includes several new and refined provisions that enable countries to respond to the most pressing challenges that concern natural resource governance.

These broadly cover four thematic areas including anti-corruption, energy transition, gender, social and environmental issues, and revenue collection.

In her foreword to the EITI Standard, EITI Board Chair Rt. Hon Helen Clark affirms that it "helps increase the relevance of EITI implementation to countries and advances open and accountable management of natural resource within a shared responsibility framework across all stakeholders.

* Go here for the link to new standard.

Ransomware criminals constantly evolving behaviours

RANSOMWARE criminals are made up of fragmented threat actor groups that are constantly evolving attack methods and approaches, which alongside other key shifts in behaviour have concerning implications for organisations in many sectors.

These are among the findings by Kroll in their Q1 2023 Threat Landscape Report.

Kroll observed a 57 percent increase in the overall targeting of the professional services sector from the end of 2022. Ransomware propelled this increase as the sector, particularly legal firms, was the most likely target of extortion and encryption attacks in Q1.

Overall, ransomware accounted for 30 percent of Q1 cases and 26 percent of email compromise cases, both remaining closely aligned with the 2022 levels.

In Q1, Kroll noted a 56 percent increase in the number of unique ransomware variants observed. While well-known ransomware-as-a-service (RaaS) operations such as LOCKBIT continue to dominate the ransomware landscape, Kroll observed a number of lesser-known variants during the quarter.

Some of these were new but others were established groups that had not been observed for several quarters.

The rise in these lesser-known variants, specifically ones such as XORIST, highlights the number of independent attackers conducting ransomware operations outside of the established RaaS groups.

Phishing continues to lead the pack when it comes to initial access across all cases. Drilling into ransomware cases shows that legacy vulnerabilities such as ProxyShell and Log4j are more likely to be exploited to gain a foothold into the system.

No matter how actors get into a network, data around toolkit deployment during the Kroll Intrusion Lifecycle indicates that actors are using exfiltration tools as standard across a wide variety of threat incident types.

As such, enabling organisations to detect actions within a network that denotes staging for exfiltration may help stop attackers in their tracks.

Threat Incident Types

In Q1 2023, Kroll observed that ransomware and email compromise continue to be the most impactful threats against organisations. Kroll also noted a rise in web compromise, most typically against the retail sector, highlighting that threat actors attack for financial gain.

Malware Threat Trends

In Q1, Kroll observed an increase in all but one of our tracked malware or malicious tool families across our active cases and OSINT collection.

Kroll detected an increase in the use of SLIVER, a cross-platform adversary emulation framework and among one of the growing numbers of public, open-source C2 frameworks, although relatively new to the scene.

Due to the public, open-source nature of this tooling, Kroll predicts SLIVER and other similar frameworks will continue to be deployed in more campaigns by threat actors.

Ransomware Activity – Independent Attackers Taking a Leaf Out of the Established RaaS Playbooks

Although large RaaS operations such as LOCKBIT dominated the ransomware landscape in Q1, Kroll also observed a 56% increase in unique variants from the previous quarter. This rise in unique variants included new variants such as CACTUS, DARKSKY and NOKOYAWA, and others familiar, but not observed in several quarters, such as XORIST and RANSRECOVERY.

Kroll has identified an increase in “one-off” ransomware variants that tend to use well-known builders. While these incidents do not typically include data exfiltration and do not extort through the threat of data release, it is likely that a server will be encrypted.

A ransom note is created which details a contact email address, an amount of cryptocurrency required for decryption and an extremely short deadline for a response.

Kroll has observed a number of XORIST-based encryptors that enable the threat actor to create a unique file extension. This builder, along with video tutorials, is available online. Initial entry is normally provided by an exposed remote service or a common vulnerability.

It is likely that the increase of these incidents is in part due to several of the RaaS groups being dismantled and the ease of entry to conduct encryption. As access is not provided by a RaaS group, typically the threat actor does not explore the network as widely as a traditional ransomware actor and may only encrypt the server where they landed.

* *The report can be found here.*

AI distracting businesses as cyber risk intensifies

SPECIALIST insurer Beazley has published its latest Risk & Resilience report: Spotlight on Cyber & Technology Risks 2023 which indicate, among other things, that boardroom focus on cyber risk appears to be diminishing despite the threats posed by cyber attacks.

The data shows that the perceived threat of cyber risk to global business leaders peaked in 2021 (34 percent) and over the past two years, the risk perception has dropped by 27 percent. Next year, it is predicted to remain at 27 percent whilst business preparedness for this risk continues to decline.

Is business becoming dulled to the cyber security threat?

As cyber fears decrease, the technological risk landscape has fragmented, with executives nearly as concerned about the perceived threat posed by disruptive new technologies, such as AI, as the risk of cybercrime.

Failing to keep pace with technology and adapting to new innovations is an issue that 26 percent of global business leaders identified as their key technological concern, yet resilience to this threat is on the decline and more than a fifth (21 percent) of all businesses feel they cannot maintain the pace of change.

Leaders are also turning their attention to other concerns such as the risk of theft of their intellectual property (IP) with 24 percent of business leaders ranking it as their top risk in 2023, more than double what it was in 2021 (11 percent).

IP theft has also become the cyber and technology risk for which businesses across the world feel least prepared, with more than one in four businesses (26 percent) reporting they feel ill-equipped to mitigate this risk.

Small business is highly exposed to cyber risk

Despite overall concern around cybercrime tracking downwards, small and medium sized businesses (SMEs) are increasingly aware of their limited ability to mitigate cybercrime threats and Beazley's data suggests they feel more exposed than ever.

Companies with an annual revenue of US$250,000 to US$999,999 report feeling less prepared to deal with cyber risks in 2023 (76 percent) than they did in 2022 (70 percent). The report outlines how cyber hacking groups are becoming more specialised and diversified, with some groups now using SME's security systems as a training ground for novice cyber hackers to learn their trade.

Paul Bantick, Group Head of Cyber Risks, Beazley said, "Business leaders are finding it a struggle to keep up with the constantly evolving cyber threat. But worryingly they appear less concerned by cyber risk than a couple of years ago. This could be because they have been lulled into a false sense of security as the War in Ukraine led to a temporary reduction in the ransomware threat level when a number of cyber gangs splintered, but this situation is only temporary and should not be viewed as the new normal."

As the MOVEit hack has proved, bad actors are always looking for new ways to attack with tactics ranging from third party supplier attacks to more sophisticated social engineering and phishing attack techniques.

Businesses of all sizes and across all industries cannot afford to take their eye off the ball, just at a moment when cyber criminals are starting to look to make up for profits lost over the past 18 months.

Paul continued, "The emergence of AI and other tech innovations as well as the increase in concerns over IP theft are now front of mind for many business leaders globally. These threats are fast evolving and unfamiliar, with many companies being caught on the back-foot when dealing with the risk. For the insurance industry, working with clients to help them tackle these challenges is vital to ensuring businesses operate in as safe an environment as possible. We need to continue to work with our clients to explain how they can improve their resilience to cyber and technology risks and encourage them to adopt a defence in depth risk mitigation strategy."

THE Asia/Pacific Group on Money Laundering (APG) has recently launched the APG Virtual Asset (VA) and Virtual Asset Service Provider (VASP) Network for public sector representatives of APG members and observers to share information on challenges, enforcement activities, experiences and policy developments relating to VAs and VASPs.

The Network will also facilitate discussions on relevant policies and papers issued by the Financial Action Task Force concerning VAs and VASPs and any technical assistance requested by APG members relating to the implementation of Recommendation 15.

The first Network meeting was held on 11 May 2023 and was attended by over 70 representatives who openly shared their experiences in areas such as risk assessments, supervision and enforcement.

It was a positive indication of strong collaboration and information-sharing amongst APG members and observers. The Network intends to convene four to five meetings for the remainder of 2023.

Reed Smith launches cyber insurance claims report

GLOBAL law firm Reed Smith has launched Cyber insurance claims: Minimize risk, maximize recovery, a report written by its policyholder lawyers.

The report examines key cyber and ransomware insurance issues, including the measures a business should take before a cyberattack and the steps needed after an attack to capitalise on insurance coverage.

The report features a series of articles, tips, updates, checklists and Q&As focused on preparing for, preventing and responding to a cyberattack, as well as what insurance coverages to review.

The report includes the chapters and topics on action and steps that can be taken to prevent an attack, prepare for an attack and best practice following an attack.

The report says that as cyber risks proliferate worldwide, adequate cyber insurance and other risk mitigation mechanisms increase in priority. *Fortune* magazine reported that the global cyber insurance market is projected to grow from $12.83 billion in 2022 to $63.62 billion in 2029.

It is expected that cyber insurance premiums will increase commensurately with the increased market demand for cyber insurance. For example, premiums for cyber coverage increased by an average of 28 percent in the first quarter of 2022 compared with the fourth quarter of 2021, according to the United States' based Council of Insurance Agents & Brokers, an association for commercial insurance and employee benefits intermediaries.

It is anticipated that new cyber insurers will enter the market, as already seen with the March 2023 launch of Intangic MGA, a managing general agent based in London that offers cyber parametric coverage.

The report also said that policyholders should pay close attention to courts' evolving interpretation of cyber insurance policies and to the developing changes in the insurance market, in general, with respect to cyber coverage.

The report further provides a brief look at several standout legal developments in cyber insurance over the past year, including from United Kingdom, United States and Australia.

Dutch database exposes hacking in maritime sector

RESEARCHERS at NHL Stenden in the Netherlands have launched a database that exposes cyber hacking in the worldwide maritime industry.

The Maritime Cyber Attack Database (MCAD), a database of incidents involving the worldwide maritime sector contains over 160 incidents.

Researchers were led by Dr Stephen McCombie, Professor of Maritime IT Security at NHL Stenden University of Applied Sciences.

The incidents in the database demonstrate the relevance of cyber security across the board of today's maritime industry and the vulnerabilities that exist.

Drawing from open-source information, the NHL Stenden's Maritime Stenden's Maritime IT Security research group collected information on over 160 cyber incidents in the maritime industry for the MCAD. The database not only covers incidents impacting vessels, but also ports and other maritime facilities worldwide.

Now available publicly online, the research group expects the database will help improve cyber security awareness in the sector and provide data for further research and more accurate simulations in this critical area.

One incident in the database includes an insider attack by a systems administrator on a United States nuclear aircraft carrier at sea in 2014 and a 2019 ransomware attack on a large container ship that prevented it from entering New York harbour.

Considering over 90 percent of the world's cargo is transported by ship, the incident demonstrates an especial weakness concerning the Global Maritime Transportation System (GMTS), the researchers said.

The role of GMTS in the global economy is significant and its security all the more essential, and yet fleets and the technology they carry are aging rapidly and becoming increasingly vulnerable to cyber attacks such as the ransomware attack in 2019. In fact, 38 percent of oil tankers and 59 percent of general cargo ships are more than twenty years old making the criticality and fragility of supply chains acutely clear.

One of the uses of the database is to develop maritime cyber incident simulations that are realistic and relevant so that companies, organisation, ports and harbours can prepare for attacks. The research group will also use MCAD to produce reports and research papers showing trends and the results of detailed analysis on subsets of the data.

Cybercrime

EncroChat take down leads to €900m criminal funds seized

THE dismantling of encrypted EncroChat communications tool that was widely used by criminals, has so far led to almost €900 million in criminal funds seized or frozen and over 6,500 arrests.

Three years since being shut down, investigators managed to intercept, share and analyse over 115 million criminal conversations, by an estimated number of over 60,000 users.

This result is detailed in the first review of EncroChat, which was presented today by the French and Dutch judicial and law enforcement authorities in Lille.

The dismantling of EncroChat in 2020 sent shockwaves across organised criminal groups in Europe and beyond. It helped to prevent violent attacks, attempted murders, corruption and large-scale drug transports, as well as obtain large-scale information on organised crime, with 197 of those arrested classified as High Value Targets.

The information obtained by the French and Dutch authorities was shared with their counterparts in EU Member States and third countries, at their request.

Based on accumulated figures from all authorities involved, this led to the following results, three years after the encryption was broken by law enforcement, and include;

- €739.7 million in cash seized.
- €154.1 million frozen in assets or bank accounts.
- 971 vehicles seized.
- 271 estates or homes seized.
- 83 boats and 40 planes seized.

Investigations into the alleged criminal conduct of the company operating EncroChat were restarted by the French Gendarmerie Nationale in 2017, after discovering that the phones were regularly found during operations against organised crime groups (OCGs).

Subsequent investigations established that the company behind the tool was operating via servers in France. Eventually, it was possible to place a technical device to go beyond the encryption technique and obtain access to users' correspondence.

A case was opened at Eurojust in 2019 by the French authorities. In the first instance, data was shared with the Netherlands, which led to the setting up of the JIT in April 2020. Since then, information on criminal activities was shared with national authorities within and outside the EU, at their request. In view of ongoing investigations, Eurojust and Europol cannot disclose a full list of authorities involved.

EncroChat phones were presented as guaranteeing perfect anonymity, discretion and no traceability to users. It also had functions intended to ensure the automatic deletion of messages and a specific PIN code to delete all data on the device. This would allow users to quickly erase compromising messages, for example at the time of arrest by the police.

In addition, the device could be erased from a distance by the reseller/helpdesk. EncroChat sold cryptotelephones for around €1,000 each, on an international scale. It also offered subscriptions with worldwide coverage, at a cost of €1,500 for a six-month period, with 24/7 support.

The illegal use of encrypted communications continues to receive major attention from judicial and law enforcement agencies across the EU. OCGs communicating via encryption were dealt another blow in March 2021, following the dismantling of the SkyECC tool.

Both Eurojust and Europol remain at the disposal of national authorities in case further support is required regarding encrypted communications by criminals.

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

Helping Business Stay in Business since 1981