

BUSINESS RISK UPDATE - SUMMER 2021

Welcome to the latest edition of 'Business Risk Update', the newsletter from KCS Group Europe specifically for our clients and partners to provide you with a snapshot of latest news and articles from the business. Like many other businesses the world over, the KCS Team is currently working remotely, and remain fully operational to service the needs of our clients and their customers.

KCS Announces formation of its business Advisory Board

KCS Group Europe today announces the formation of a new Advisory Board, dedicated to supporting the work of the Group as it continues to both grow in key markets worldwide and excel in carrying out challenging and complex assignments. Mr. Andrew Love will chair the Board, and he will be joined by three of the UK's leading business luminaries: Lord Tim Clement-Jones CBE, Rt Hon Brian Wilson CBE, and Ian Thomas OBE.

Together, this Board will be dedicated to exploring new opportunities in global business, making use of their considerable collective body of knowledge and experience. Ever since its formation, KCS Group Europe has 'punched above its weight' in terms of the Clients it works for, the depth and breadth of its investigative and intelligence-gathering capabilities, and the ultimate value it offers. Forming a Board with such a diverse yet complementary skillset, is the next logical step in ensuring that KCS Group Europe continues to go from strength to strength.



[To read our full announcement please click here](#)

Political Risk Advisory Briefing: United Arab Emirates — Energising The Future

This latest Political Risk Advisory Briefing from KCS focuses on The UAE. The United Arab Emirates have a Risk Rating of 4.5 (Very Possible, tending High)

Think of the Middle East, and you think of oil. Whether it is Saudi Arabia's \$230bn USD yearly revenue through Aramco, Iran's constant battle over sanctions, or Iraq's struggle to rebuild itself through oil after the war, the modern Middle East is inextricable from petroleum. This has been both a blessing and a curse: the region has seen unimaginable economic boosts as a result of its oil wealth, but also deep-rooted corruption as a direct consequence of the resource.

Nowhere is this better illustrated than the United Arab Emirates: where the Burj Khalifa rises as the world's highest manmade structure as a testament to what the UAE has become. 'Dubai' has become a byword for exotic luxury and business, where you are just as likely to find an influencer or Premier League star on vacation as some of the world's leading industrial and financial offices.

But underneath the surface, corruption, nepotism and political problems present an uncomfortable reality that the oil & gas industry, for so long the UAE's biggest source of revenue, both defines and is defined by.

This platform of economic diplomacy arguably sets the tone for the entire UAE market at the moment. It is going bigger and deeper in terms of the oil & gas opportunities and investment, broader in the scope of 'energy' ventures in the first place, and even more global than before in terms of the kinds of relationship it is seeking with foreign companies. All of this combines to confirm (as if there were ever any real doubt) that the UAE's relationship with extractive industries is as firm as ever, and that diversification is at present a 'spin-off', rather than the main event.

The time is now for firms both making their first steps into the market, and those already established within it, to

take stock of their position and, with the appropriate diligence & support, to make themselves as integral to the oil & gas industry, as the industry is to the UAE.

In this latest Political Risk Advisory briefing on The UAE, we have focussed on five areas:

- **Diversification?**
- **From The Ground Up**
- **An Earthbound Gas Giant**
- **Threats**
- **Political Matters**

[To download a copy of our full report, please click here](#)

KCS Team News ...

Despina Mooney joins KCS as Analyst Intern

KCS is delighted to announce Despina Mooney has recently joined the team as Analyst Intern.

In her new role, as a member of the Intelligence Department, Despina will conduct investigation and analysis on all manner of due diligence, tracing and counter-fraud cases.

She will also play a role across multiple areas of the company, particularly in providing a dedicated cyber-liaison between the Intelligence and Cyber Services teams to enhance Intelligence work in the cyber area. In addition, Despina will also be involved in securing new business and promoting the added-value propositions of KCS to its clients.

Despina has recently graduated from Liverpool John Moores University receiving a BA (HONS) in Policing Studies and alongside her role at KCS will continue her studies to achieve an MA in Covert Investigations & Specialist Intelligence.



Sam Whitmey promoted to 2 I/C Intelligence

Congratulations to Sam Whitmey who has been promoted to the role of 2 I/C Intelligence Department - Lead Intelligence Analyst.

Sam joined KCS's intelligence team as a Junior Analyst in November 2018 following completion of his studies at The University of Bristol where he achieved a 2:1 in Russian & Politics. This promotion reflects his value to the company over the last two years and the regard in which his skills are held. We look forward to him developing his career further with the business in the years ahead.



Ransomware is still the big news in Infosec but recent geo-political developments and the weakening of Bitcoin as a means of ransom payment, may cause a change in tack by threat actors.

President Biden's meeting with Vladimir Putin in June signalled what appears to be an agreement to extradite threat actors responsible for attacks, though whether it was window dressing, or a real commitment is yet to be seen. The additional threat of a US military response to counter attacks against targets of national importance is certainly a shot across the bows of states that sponsor ransomware groups.

Yet ransomware attackers are evolving. Rather than targeting anyone and everyone, going for low-hanging fruit no longer seems to be the modus operandi. Recent trends certainly point to a move away from the in-place data encryption and ransom demand to a data deletion/encryption and exfiltration model, aimed at larger targets with valuable information, which are likely to pay larger ransoms.

Many analysts believe this is likely to be more aligned with the goals of the Russian state.

So, what of the crypto connection? It seems undeniable that crypto currencies have emboldened attackers by making

ransom payments more difficult to trace to threat actors, but the news that the Binance cryptocurrency exchange had assisted law-enforcement in fingering and taking down the FANCYCAT criminal group in Ukraine, through the analysis of patterns recorded in the blockchain is an interesting development.

Cyber criminals need to launder their funds before they can extract them to buy goods safely and it seems that in this case, they created a complex network within the Binance crypto exchange to pass coins back and forth, in an attempt to wash away any trace of where they originated.

In this case, analysis of the blockchain and the use of complex detection and Anti Money Laundering techniques allowed Binance and a number of specialist block-chain analytics companies to work together with law-enforcement to identify where the funds were being "cashed out".

Regulators don't think exchanges are doing enough to combat money laundering – Binance itself was banned from regulated activity in the UK by the FCA. Expect more exchanges to either up their game in eliminating money laundering from cyber-crime or suffer the consequences.



In case you missed it ...



[The body corporate](#)



[No Mr Bond, I Expect You to Pay!](#)



[A New Scramble for Africa?](#)



[Political Risk Advisory Briefing: Kenya May 2021](#)

To subscribe to regular updates from KCS Group Europe, [please click here](#), if you no longer wish to receive business updates from us, please [click here](#) to unsubscribe