KCS Group Europe

BUSINESS RISK UPDATE - SPRING 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.

What to look out for in 2021 - a Coronavirus free, intelligence focused view

After the overwhelming year that was 2020, with the prospects of World War 3 between USA and Iran almost becoming a reality, Australia on fire and the elephant in the room that is Covid-19, 2020 has definitely been the most chaotic year in recent memory. Now that some countries like New Zealand are "Corona free" and others like USA, UK and Russia are rolling out vaccines, the hope is that 2021 is the year we can go back to normal. What that exactly means is uncertain as of yet, but the most common expectation of 'normal' is pre -COVID-19 times. With that being said, 2021 should see some interesting developments in the world from an intelligence point of view. This is by no means an exhaustive list; however, more a matter of raising awareness of the key developments that businesses should be keeping an eye on.

The first and possibly the most intriguing aspect of 2021, is in how President Biden's foreign policy will affect the world: already he has distanced himself from Donald Trump by, among other things, re-joining the Paris Climate Accord and the World Health Organisation, and lifting the ban on Muslims from seven nations entering the United States (and the 'wall' will remain unfinished, too). The bigger questions remain: how for instance will Biden look upon rejoining the Iranian nuclear deal, and will he seek to continue or dismantle the legacy of the physical meetings between Trump and Kim Jong-Un? A 180° pivot from Republican positions would be considered standard, but with Biden, the watchword may very well be expected to be 'calm' after four years of Trump and he might not be as bold as one would expect – at least, not in the short-term. "America's place" is a very different mission statement from "America First" and while on the whole a sensible one, it could arguably embolden those parties who see things only as a zero-sum game, and reason that if America is no longer openly hoping to be First, then the gap will need to be filled.

One thing that Biden – and the world – cannot ignore is the ever-growing threat of Russia. Putin's foreign policy since 2014 has essentially been to promote anti-western sentiment, interfere in Western elections and affairs and generally be a thorn in the West's side. In the past Biden has been critical of Russia to say the least, having described Russia as "the biggest threat to the United States." He has also described Russia as "a country in enormous decline, and a second-rate military power, unable to compete with the West, and a kleptocratic regime run by KGB thugs".

How is this to affect western businesses in Russia? Well, usually after a political fallout with the West, Western firms in Russia have suffered from the Russian government directly interfering in their businesses' affairs. For example, in 2014, after the sharp deterioration in U.S.-Russian relations over the conflict in Ukraine, the Kremlin sued McDonald's for allegedly violating the government's safety codes, and even temporarily closed four stores over alleged "health violations." Similarly, hours after imposition of increased sanctions on Russia that same year, authorities raided the Russian headquarters of Ikea. As a result, firms operating in or having partners in, Russia, need to be conscious of America's and the West's future foreign policy towards Russia, as any political fallout between them is likely to affect those Western businesses in some form or another. Politically speaking, Russia will not get anything like the 'free ride' from Biden that it got from Trump, and it may yet be that the domestic (and international) anger over the continuing detention of Alexiy Nalvany could yet act as the foundation for another round of sanctions and consequent 'trade war' or similar.

Russia's increasing ties with China are also likely to develop into a deeper, if not necessarily public, relationship over the coming year. The two nations are becoming closer politically, economically and military, which is one of the reasons why the Pentagon, for example, has shifted the focus of its large budget away from wars in the Middle East to a greater emphasis on the types of weapons that could be used to confront nuclear giants like Russia and China with particular focus on 'enhanced lethality… in a more contested environment'. While a full-scale military conflict may still seem unlikely, the American way is to sabre-rattle in an unsubtle manner in the manner of a silverback, ignoring both the true threat (state-sponsored cyber-attacks) and the most appropriate means of stopping them (targeted responses to threat actors rather than 'advanced high-end weapons systems').

Unless Biden refocuses US defence capabilities on irregular threat actors, it is envisaged that the US will experience a large-scale and highly damaging cyber-attack before the year is out, and both Russia and China are likely to privately challenge the Israeli dominance of international cyberspace.

This is not without credibility, over the past few years both Russia and China have been launching large- and small-scale cyber-attacks all around the globe. Even as recent as January 2021, Russian and Chinese hackers allegedly hacked into various entities of the Dominican government. The threat is real – and in a divided and damaged world, there are few better times for the bad actors to move.

In the Middle East, the situation is just as volatile as ever. In late January 2021, Saudi Arabia was feared to have come under attack as large explosions were heard over the capital of Riyadh. It is reported that the explosions were intercepted missiles, launched from Iraqi militias backed by Iran. This Cold War between the two nations is becoming more violent by the day, and now that the pro-Saudi Trump administration is gone, we may see an Iran which is more willing to take more risky, potential fatal military actions against Saudi Arabia and its proxies. Were it not for the coronavirus pandemic, after all, the state of tension that existed between Iran and virtually every other nation in January 2020 after the assassination of Soleimani,

the downing of Flight 752 and the strikes on US airbases, may have developed into an all-out regional conflict. Unless Iran is brought back into the international fold through virtue of the JCPOA or similar (once again, no pressure, Joe Biden), it is projected that she will become an increasingly unilateral and unpredictable actor and what starts in Iran will almost certainly embroil the whole Middle East, to say nothing of proxies and third-party states with an interest in the region. Moreover, if the overtures of some sort of formal rapprochement between Israel and a Saudi/Emirati coalition develop into a full-blown symphony, then Iran is likely to be regionally isolated even further and would be likely to step up its attempts (along with covert international support) through cyber-attacks in particular, to restore its own superiority. This means that any firm in the area risks becoming collateral damage and thus must keep up-to-date with all political developments, particularly those not making the news, in order to feel confident in their position.

Lastly, one thing that UK companies should be look out for from an intelligence point of view is Brexit. As the true impact of Brexit is yet to be revealed, particularly in the light of corona, it may be thought that little will change from an intelligence perspective, but this is not the case. A likely consequence is that the UK will become a favoured destination for tax havens, free ports and other unsavoury practices on the part of unsavoury individuals, bringing business to the UK with the true intention of laundering 'dirty' money and taking advantage of a more permissive system. Therefore, due diligence on the home front takes on an even greater degree of importance, as the very operating environment has changed and not for the better, in terms of security and business confidence. While the UK itself joining 'blacklists' of tax haven nations might be far-fetched at present, there is a real chance that she will do nothing to either deny havens a foothold on these islands, or attempt to stamp out the problem elsewhere (in the BVI, for instance). Businesses in the UK thus have a much broader threat picture with which to contend.

All told, the 'new normal' that 2021 promises cannot be pinned down with any great certainty, such are the shifting tides of political, economic and social spheres in this year even more than any other. But the general trends point to a much deeper, and broader, set of risks across the board, from the same sources as have always been dangerous, that will have a major impact on almost any business venture. If anything can be said to be 'normal', it is that some threats – and some actors – never change.

New Network Perimeters

Traditionally, IT Departments have looked to secure their network perimeters with devices like Firewalls which control the flow of data between the private enterprise and the public internet. Once employees were in the office, they were safe (or as safe as can be).

In 2021, how many employees are sitting in safe and secure offices and how many are working from home on a personal, unmanaged broadband connection? The network perimeter has moved and the "attack surface" is vastly more intricate and complex.

IT Departments have far less control over an employee's home security than they would over the office firewall sat next to them in the comms room; was the remote workers router password changed from "admin" to something secure when it was first set up? Has the router had security patches applied regularly? Is the wireless network secure? Is there a potentially unsecure and malicious "smart" device connected to the same network that an employee is using?

KCS have seen "threat actors" shifting their focus away from office networks to points of entry that do not necessarily fall under the control of IT departments. An "always on" corporate VPN can help but we have seen vulnerabilities associated with a number of enterprise class Firewall VPN products over the last few months.

So, what can be done? Well, the first thing to do is to take the issue seriously and devise a policy that ensures employees only connect via a guaranteed secure connection – no secure connection, no ability to access work data; ensure that employees have followed basic security standards with regard to their own home networks… and then audit them. It is time consuming but vital to check that they have implemented these baseline standards and you can be sure that some of the less technically minded employees will have misconfigured them – you are protecting your corporate network perimeter and therefor your corporate data. By happy coincidence you are also potentially protecting your employees and their families when they are not working.

Corporate Email – how much is too much?

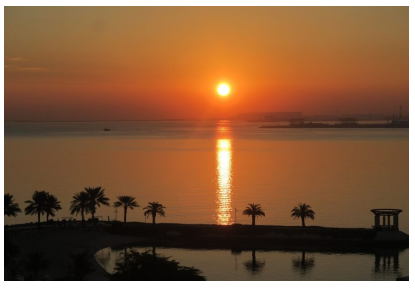
Talking of corporate data, the recent "Hafnium" Microsoft Exchange attack is genuinely concerning. If like many companies, yours is running an on-premises Exchange server, it needs to be patched but you also need to make sure it's not already been breached and something nasty has been installed for future use. KCS believe that ransomware groups could exploit this situation in the coming weeks, so ensure that there are clean, offline backups…

This breach further raises the question of just how much data do you need to make available? Do users need email going back 10 years to be available at the drop of a hat or can they make do with 6 or 12 months? Offline archiving potentially reduces the amount of data that is available to steal and the subsequent tricky conversations required, when informing customers that you have been breached and emails that they sent to you are potentially being pawed over by criminals.

KCS predict a rush of migrations from on-prem Exchange to cloud services like Microsoft 365 in the coming months as a result of this. Migrating from traditional on-premises models to hybrid or cloud M365 throws up its own issues, however it is also a really good opportunity to take stock of the current infrastructure configuration and to dramatically improve security and resilience, just make sure that the migration is properly planned and documented and that IT use an experienced architect to get the configuration nailed down. Getting M365 right from the start will greatly improve security down the line.

In case you missed it …

Icebox of delights



Qatar: New dawn or false dawn?

Andrew Love F.C.A announced as Non-Executive Chairman

Virgin on the ridiculous

Telephone: +442072451191 **Email: info@kcsgroup.com** **www.kcsgroup.com**