

## BUSINESS RISK UPDATE - SPRING 2020

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 you will see in this edition of risk update that we have included a couple of articles directly focussed on Covid-19.

### Threat increase during times of crisis...

**Following the recent pandemic announcement and the increase in the numbers of people working from home, it is important to ensure that alternative procedures are put in place to enable businesses to continue to operate in the medium to long term.**

It is during times like these that incidence of attack increase. External threat actors are likely to seize on opportunities relating to confusion associated with the change in normal internal company communications. Likewise, the enforced use of employees' personal devices opens potential for attack through poorly configured security.

What's more, the risk from Internal Threats also increases as perceived job security decreases.

There are a number of factors which KCS recommends are implemented to ensure your workforce have secure access to their data;

- Establish secure connections using a Virtual Private Network.
- Implement Multi-Factor Authentication to guard against phishing/account takeover.
- Regularly check Audit Logs for evidence of data leakage/theft.
- Provide employees with properly secured, monitored and managed devices.
- Ensure policies are in place and staff are aware of their meaning.

- Be hyper-aware and alert to anything suspicious – if something doesn't look right, speak to your colleagues and staff about it on the phone, rather than rely on email.

KCS has noticed that Threat Actors are exploiting the pandemic to gain access to system login details and web portal credentials, with a view to collecting sensitive corporate intelligence. Now is the time to be vigilant, employees are working from home which means they're operating in a new, unfamiliar environment making them more susceptible to social engineering. What's more, System Admins may not have access to their usual tools and resources, so auditing may not be being performed properly and breaches may not be flagged. This adds up to a significant increase in the threat to your Corporate Intelligence.

For more information, please contact the KCS team. [info@kcsgroup.com](mailto:info@kcsgroup.com)

### Somalia: A Shining or Fading Star?

**After almost fifty years what was once a remote pipedream seems close to reality. Somalia is set to for the first time in half a century to hold a "one person one vote" electoral contest.**

The significance of this cannot be underestimated, particularly given the violence that racks the country on a daily basis and the seeming impossibility of a permanent solution. Could this be the first scene in Somalia's second act?

Since the last democratic election in 1969 Somalia has become a byword for failure and has seen the rise of terror group Al-Shabab (and local affiliates) with concomitant violence restricting effective government to the environs of Mogadishu, and an almost total moratorium from international businesses pushing the country further into the bracket of 'failed state'. While it ranks at or close to the bottom of practically every development index and variable, there is hope that the first universal suffrage election will go some way to setting Somalia back on the right path.



[Read More](#)

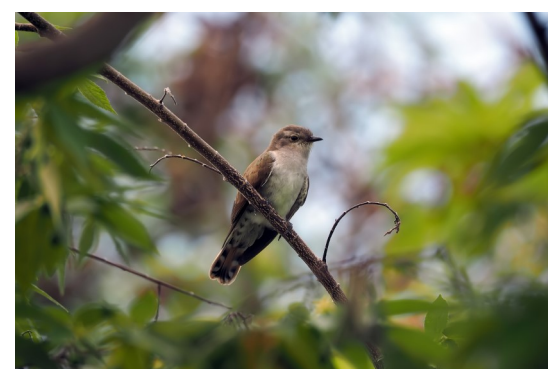
### Loudly sing Cuckoo...

**New dogs, old tricks. The Israeli military was once again recently targeted by bad actors, this time via a modern interpretation of the honey trap: individuals posing as beautiful women have been attempting to lure soldiers into downloading a compromising app.**

The Israeli line is that this is a Hamas operation, and one that they allowed to continue in order to conduct intelligence-gathering of their own, but a compromise of this nature does not look good no matter who the perpetrators or targets are.

Worse, it proves that adaptability is the name of the game for criminals – and that imposters and fakes are fast becoming the norm.

Honey traps of old would be intended to get specific information out of a specific target or create conditions for 'leverage' in the future. This attack worked slightly differently. While all of the men targeted were Israeli military personnel, there was no suggestion that they were deliberately targeted – rather, the fact that that they were military was enough. Also, the app was designed to give the hackers access to the information contained on the phones, which could be personal at best and state-sensitive at worst – and to take audio and visual records obliquely. This is very much 'the long game'.



[Read More](#)

### COVID-19...

**It is clear that the business world, like any other, will have to adjust to a rapidly, and possibly long-term, changing way of life as the Covid-19 pandemic intensifies. While the show must, as they say, go on, there will be those who seek to take advantage of the framework which Covid-19 imposes and use it as a springboard for unethical and criminal activity. Now more than ever, we should be aware, and wary, of these tricks and ensure that corporate affairs are not destroyed by bad actors trading off a new set of circumstances.**


1. The most obvious effect of Covid-19 is an almost blanket travel ban (whether imposed or advised), with no telling when this might be lifted. This therefore poses dangers to those firms looking to establish ventures and partnerships abroad: what would have been an in-person visit to, say, look over a factory site or have a personal meeting at a headquarters, is now restricted to a video or conference call. It is a lot easier for bad actors to con and misrepresent themselves via this method: being able to conceal, for instance, that on-the-ground operations are far from what was promised, or not having to live up to their untruths about the scope and scale of their capabilities. Being at a physical remove increases the chances of a bad actor being able to conclude a deal based on fabrication which should, on closer inspection, likely not go ahead.
2. For industrial companies that rely on global supply chains, or investment houses and legal firms who find traditional markets no longer as open as perhaps they would have been, there will be a need to secure alternative revenue streams as quickly as possible. But this should not come at the expense of a proper understanding of who these companies are and who is behind them - or else an already struggling business could lurch from bad to worse and find itself stuck with a rapacious, corrupt partner at the worst possible time.

3. It is undoubted that multiple firms will face financial hardships during the crisis, but some unscrupulous firms will be looking to take advantage of this. Whether it is by asking for more financing or supplies over and above what was already agreed, with-holding these for the same reasons, or pressurizing a client to take a supposedly good deal now, as Covid-19 means it won't be around tomorrow (as has allegedly happened at cruise giant Norwegian), it is worth double checking that any disruption is genuine and not purely for ulterior motives.
4. And attention must also be given towards the 'reset' of normal life, whenever this comes. If standards are lowered and practices changed for the duration of the crisis, out of perceived necessity, then these should become the norm. While there is perhaps a genuine societal conversation to be had about the degree to which the 9-5 office routine and the like remain necessary in any post-Covid-19 world, there can be absolutely no substitute for, or dilution of, appropriate diligence practices to scrutinise and gain assurances over deals and partners. No matter how the world may change after Covid-19, the only appropriate change for risk assessment should be that it becomes even more stringent than before.


**The investor Warren Buffet characterises two types of people in a crisis: those who are greedy, and those who are fearful. We will now see an influx of the greedy, looking to profit from and exploit the Covid-19 virus crisis (and those firms affected by it) as much as they can. The challenge for respectable business is not so much to be fearful, but to be cautious and sceptical even over and above the norm and manage the situation with vigilance.**

### A deeper selection of our products and services ... Please click the image for further details


KCS Group Europe  
We look at the world differently ...




How & Why We Acquire, Judge And Grade Intelligence ...


 KCS  
Strategic Intelligence & Corporate Security

Discreet Non-conventional Due Diligence (DNCCD)




 KCS  
Strategic Intelligence & Corporate Security


The Equation of Intelligence




OSINT + TECHINT + HUMINT  
= FUSION

 KCS  
Strategic Intelligence & Corporate Security

Cyber-Security, NIPS & Social Media Vulnerability Assessments



 KCS  
Strategic Intelligence & Corporate Security

**We are able to provide a comprehensive range of services in the areas of security, intelligence and cyber security to help identify, mitigate and deal with any risks which can impact businesses both financially and reputationally.**

To find out about some of the services we can offer and how we can help your business [please click here](#).

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