

The company we keep

October 2021

If we were to create an ‘alphabet soup’ of the business world, it would start pretty conventionally: CEO, CISO, CFO. Going deeper, we might find rarer ingredients: FTSE, ISO, CRM. But the most vital elements are sometimes left in the tin: DD, KYC and AML. Without them, the meal can turn sour, so why are some corporate chefs still treating them as optional seasonings



rather than vital elements? The answer lies not only in the company we keep, but the companies we are – and what people on both sides of the divide are prepared to do.

Due Diligence, Know Your Customer, Anti-Money Laundering. These are the three principles by which the continuing security of a business is built and upon which it should be founded, on the basis that a good habit is hard to break and that starting as you mean to go on is generally a good idea. And yet. Time after time stories break of firms having lost millions to fraudsters, of surface-level ‘sure hits’ being naught but smoke and mirrors – and these are just the tales we hear about. One of the few matters on which everyone can agree, when it comes to fraud, is that the scale of the threat posed is greatly underestimated.

So, the question must be asked – why on earth do we make it so easy?

Lest this be considered too inflammatory a statement, consider some examples drawn from just the past few months of projects that have crossed the KCS desk. An instance whereby a client asked for due diligence on a potential partner with no supporting information to assist in validating him – not even a passport. An instance of investigating a fraud with the client’s shell-shocked amazement that the deal could have gone wrong. And an instance where, having been told some very concerning derogatory information, the client requested this to be removed from the report that would decide the CEO’s position.

None of these are special; none of these are unique – throw a dartboard at a book of investigative firms and you will find the same raft of cases; but more to the point you would get the same issues if you aimed your dart at the legal sector, the industrial sector or the financial sector. There is a widespread corporate sickness when it comes to diligence matters, and the worst thing is that this is a largely self-inflicted malady.

Consider the first case referenced above. To not even perform the most basic verification checks, never mind anything more specialist or in-depth, is simply not a fit position to take in today's business world, and the lack of substantive knowledge about a potential hire, target or opportunity, save for what they themselves have relayed, starts the relationship off on the worst possible foot as the target subject – who may after all have fabricated his story or be himself a 'cleanskin' for political interests – is given the implication that, frankly, here is a victim that will swallow anything. In some situations,

if what the target says is acceptable, diligence might not even be instituted – a patent peril of trusting what you want to hear and not Knowing Your Customer in even the meanest sense of the word. (This does of course make the job of the professional investigator a good deal harder and costlier, with at least the second of these having an impact on the client).

In the second, such a situation would typically arise from the bare minimum of original diligence being done in-house – either against a set of criteria that minimised the likelihood of a deep-dive, or via mechanisms that are insufficient to properly deal with the task (not least because the presumed cost-benefit analysis is deemed to skew heavily towards the former).. The former could be set either knowingly, to which we shall return, or unknowingly, with the client not appreciating the full range of appropriate considerations that comprise proper diligence. The latter is an inherent fact: the databases and resources available to legal AML departments, or to investment-house partners, are never going to match the breadth and depth of capability available to specialists. There is no shame in engaging experts on any other matter – yet the stigma remains here.

But the counterpoint to this is reflected in the third example – sometimes, companies are entirely aware of the demands and requirements of due diligence and know what should be done, and deliberately turn from this path. This might be (as mentioned above) commissioning diligence to such a deliberately restrictive standard that it will be virtually useless in practice – or attempting to ignore findings that they do not like. This is easily the most dangerous position, as it implies that the diligence is irrelevant, the decision has already been made – regardless of what is found.

This question of red lines is a key one, applying as much to theory as practice. A client knowing beforehand that anything short of, for instance, sustained homicide will be a barrier to employment, or choosing to overlook issues of laundering/corruption based upon the 'standard of proof', is no different to a company choosing to rely only on sanctions-lists and criminal records.

These 'red-line' conditions are not sufficient, but companies (or the individuals within them) are either too trusting, or too greedy, to put necessary diligence in perspective. It can be reduced to a box-ticking exercise, and complacency and/or arrogance continue to push this to the fore.

Interestingly, the recent Pandora Papers leak provide an illustration of this in practice. While strictly speaking, participation in 'the shadow economy' is not outrightly illegal and there is no suggestion that the majority of those involved have acted illegally, such is the level of corruption that is enabled by the system from Britain to Bermuda, and the obvious immoral intent that comes from funnelling interests and assets to no-tax offshore jurisdictions and shrouding oneself in anonymity, that the obvious conclusions must be reached as to the true legitimacy of the practice.

And yet you will still find law firms willing to act for the most corrupt and hypocritical individuals who have been named time and time again; still find financial firms offering advice on 'tax optimisation' to those who should be contributing the most but looking to give the least. At the very least, such clients should come wrapped in orange flags, but the fact that three successive leaks have exposed more and more iniquity suggests that there is still a very buoyant market for holding one's nose – and as (again) the need for successive leaks has proven, the system enables and even encourages this activity. In these situations, the company that is kept, is deliberately permitted and even sought after – because the market colludes in, and enables, it.

There is no shame in admitting one's non-expertise in other matters and employing specialists to help and thus improve the quality or fundamental standard of the product. If you are building a house, you are going to want to employ a plumber at some point. But with intelligence and diligence the plumbing, as it were, is commonly kept in-house – hence the higher chance of self-inflicted damage. We have seen instances already as to why this might be the case: from cost to naivety to deliberate ignorance. But also, it is fair to say, unity of thought and purpose is something sorely lacking.

Few sectors have mandated rules that every entity within must follow; merely 'guidance' that leaves it up to the individual or company. This creates confusion, inconsistency, and the occasional *laissez-faire* attitude – if the corporate world in general does not care, why should/how can its constituent elements?

At its heart this is an attitudinal question for firms. Some passively do the bare minimum, some barely engage with the process, and some actively do not want to know. And the lack of hard-and-fast directives on what should be done serves only to 'muddy the waters' further and place the onus on sectors that can be either unaware of, or uninterested in, the breadth and depth of the threat.

This is why, despite the dangers out there from the company we keep, just as crucial is consideration of the threats arising because of the companies we are. A hard truth, perhaps, but one that cannot be ignored.

KCS Group Europe - Strategic Intelligence & Corporate Security

A leading provider of security and intelligence services, we operate discreetly in some of the world's most difficult environments on complex cases of fraud, theft, corruption, or market dynamics. We gather intelligence through the discreet use of human sources to level the playing field and help our clients to identify and deal with any risks, weaknesses and threats which could impact on their business financially or reputationally.

Our key areas of expertise include:

- Corporate Intelligence Services
- New market or sector entry research
- Know your customer screening

In addition, through our specialist team at KCS IS, we also offer a unique service in the areas of Cyber Security and Cyber Risk. This covers penetration testing, vulnerability assessments, intelligence gathering and cyber security audits, providing unparalleled, analysis, contingency planning, and implementation for our clients.

**To find out more or to arrange a meeting to discuss your business needs, please...
email the team at info@kcsgrroupeurope.com or call (00 44) 207 245 1191**
