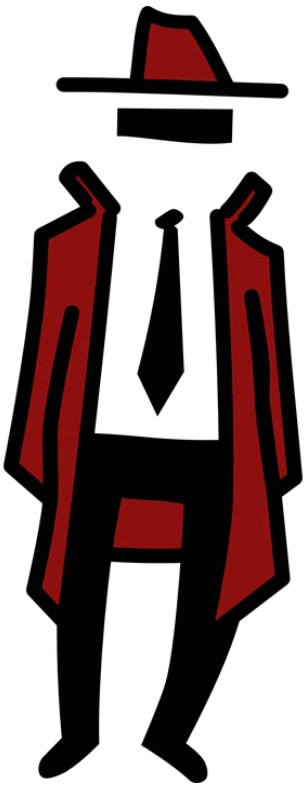
KCS Group Europe

A Decade of Intrigue

February 2018



This week, KCS Group Europe is celebrating 10-years of business. During this time there has been great political upheaval in practically every continent around the world, global shifts in the social and economic systems from the 1% to the developing world, and a whole new range of threats has arisen – not least from the cyber-realm. As we look back over the past ten years, it is clear that although there have been great advances in attitudes and approaches to holistic security, there is still a tendency to remain "one step behind" the bad actors – which in this industry, can be the difference between failure and success.

The Spanish Prisoner has a new descendant

The confidence trick of impersonation, with a sob story, is one dating back to the 1600s where a representative of a 'Spanish prince' would ask for money to help release his master – money which would of course see a sizeable return once the royal person was free. There was of course no Spanish prince, but a lot of red faces from those who fell for it (presumably the ancestors of those who would go on to buy the Brooklyn Bridge a hundred times over). This particular con saw experimentation with the form in the 20th century, with Nigerian princes and astronauts being the favoured fleeces. But as people have become more attuned to these kinds of scam, the bad actors have made an evolution. They are now playing their laments against very specifically chosen individuals, and they are making their attempts devastatingly plausible.

Consider, for instance, a recent Middle Eastern prince arriving in London with a retinue, limousine, palatial suite and the sole intention of rinsing £50,000 out of one specific client. He was of course nothing of the sort: not a prince (not even an Arab) and with all the trappings of power merely creating an image. But he almost got away with it (and this would not be the first time this exact individual had pulled a stunt like this). Unlike the Spanish Prisoner or Nigerian 419 scammers, this individual jumped straight over the credibility gap. Not only did he look and sound the part, but he could (seemingly) back it up – an investment of £20,000 had already been made last year to the intended victim to lay the groundwork.
Of course, the fact that the limousine and suite were on credit and their occupant would disappear before the bill was presented was not something that the clients needed to know.

In this particular case, the fraudster was identified before he could do extreme damage to the client, but he had conducted at least half a dozen similar successful operations throughout his career. All were built on the foundations of plausibility, believability and specialty: all of which trigger naturally trusting responses in our brain and none of which could be said about former scams. This is the way that long cons are moving now, and defences are being let down as a result.

Criminals now cross continents

As may be expected, the rise of the Internet and the spread of globalization has led to developments in crime, most prominently in how technology allows disparate groups to work and communicate on complicated scams without ever having to meet each other. Sometimes this can be led by the state (see below) but most commonly, it is exploited by private gangs.

Numerous cases that have come across our desks in the past decade have involved the initial villains, or at least the first group identified, as being just the tip of the iceberg. We have seen a fraud directed from Iran

using Bulgarian hackers as intermediaries and British individuals as recipients of the stolen money; we have seen a Caribbean travel company targeted by Russian hackers hiding behind middlemen in Cyprus; we have seen a case of identity fraud controlled by family members in Jordan but using various teams in Kazakhstan, Nigeria and the UK to each perform one part of the whole.

Not only has this introduced the 'core conspirators' to exploits and attacks which by themselves may have been impossible to conduct, it also puts layers between them and the source of the crime. You may be able to trace your stolen money to a bank in Bulgaria but finding out that it then went to Iran is a good deal harder. In this way the cons are designed to be concentric: the 'wheels within wheels'. This means that investigations must get deeper and broader – or they risk missing the key criminals entirely. That so many of these 'webs' avoid being broken up, by virtue of their secrecy, is not lost on the criminals of today.

Onions!

An old joke around the fall of Communism went, why are Russian buildings shaped like onions? Because the more layers you peel away, the more you start to cry. While slightly humorous there is actually a dark heart behind this jest. It is frequently the case that what is on the surface does not only not tell the full story, it might not even be part of the story at all.

"Fake news" has been a buzzword in recent years and there is no doubt that fake narratives are peddled in the geopolitical arena in attempts to swing sentiment a certain way. However, this is also true in business. Potential clients/partners/merger targets can have secret (compromising) pasts they may not want to reveal, they may be put up as 'puppets' by more insidious interests in their country. A persons reputation can be cleaned online, and all negative references removed, records can be altered and removed, and certain individuals can be thrust to the fore not because of their great qualities, but because someone wishes to remain behind the curtain.

This can be either on the 'micro' scale or the 'macro' one. A one-layer onion would most commonly be seen where a particular figure of bad repute cannot be openly seen to be involved in a situation, so a front man (one with a deliberately clean reputation) is deployed to assuage any fears about the enterprise and keep the bad actor in the background.

However, this does not preclude the bad actor from playing an active role – one that a client may not even be aware of. In a similar vein, a multiple onion would see not just many individuals put up in place of the true master of puppets, but also multiple smokescreen companies and trusts as part of the corporate web to hide the true picture. (This latter has been personally seen on many occasions on the behalf of Iran's Revolutionary Guard, who are contentious to say the least). Knowing who you are really doing business with has never been so difficult – or so vital.

Lasers, not shotguns, are the weapon of choice

Cyber-scams have become as evolved and intelligent as technology – and the naivety of victims – allows. No longer do people get taken in by Nigerian princes with vast sums to give who have inexplicably chosen them as a recipient. What we have seen now is an almost total (by the dedicated scammers) move from shotgun approach (firing out a thousand generic mails and hoping one hits) to laser targeting: choosing a specific target, employing a high degree of social engineering and research to convince them, and then guessing (often correctly) that the victim will be far more likely to fall for a scam specifically tailored to them.

Not only does this confer a higher degree of suspicion and concern for communications in every-day usage – can you be sure if the latest email from your Finance Director is really from them? – but demonstrates the 'seriousness' with which this kind of operation is now being undertaken. It is but the work of a moment to

prepare a 419 email with little hope of a return. But carrying out what can be extensive social engineering and research on a dedicated target is a time-consuming venture, with an appropriate expectation of success. The hackers are getting a lot more serious.

The same applies to the greater degrees of industrial espionage. While outside hacks do still take place, it is far more common for inside men to play the system to their advantage or social engineers to elicit sensitive information from specially chosen targets. The biggest cyber-vulnerability is still the one sitting between the chair and the keyboard.

New horizons come with old threats

Justifiably or not, there are some jurisdictions that instantly put one's defences up. Russia, Iran, China, Nigeria, to name but four – these are markets where business sentiment does not feel particularly positive. Whether it be down to the corruption in the system, a constraining bureaucracy, an untenable security situation or any other reason, firms can sometimes get cold feet about difficult jurisdictions and prevent their business from expanding and growing as a result.

Such an attitude should not be discouraged. There are of course numerous threats in all of the above, and more, and caution should always be applauded. But too much caution, a head-in-the-sand approach, means missing out. Likewise charging in and partnering with local individuals/companies on trust, or with inadequate due diligence, will bring nothing but risk and worry to all concerned. How does one find the middle ground?

Companies introduced to the Russian market (as an example) in recent years have all had the same issues: navigating a business environment heavily weighted towards Russians, combating the endemic corruption at practically every level, navigating the bureaucratic bodies that need to be dealt with and ensuring that competing interests with *krysha* [protection] do not get an unfair advantage. On occasion, and with each problem, a solution was found but crucially these were reliant on a deep and up-to-date understanding of the market, its dynamics and of the right approach. There is absolutely no substitute for local knowledge. And yet, companies dive in without fully understanding how they could be affected in the long-term broader picture. If there is the opportunity to get a fuller understanding, why would you not take it?

States see corporates as easy targets

State-sponsored espionage has been alive and well since the time of Julius Caesar and has, like practically everything, been given a greater lease of life through technology. The number of cyber-attacks various nations have waged against each other would easily run into the millions and even when these are not confirmed (for instance the shutdown of Saudi Aramco or Iran's nuclear facilities) they are widely accepted and cause significant damage. However, it is not always possible/feasible to attack a state entity. They are, after all, very well defended. State espionage may then turn to private companies: either as a means to an end, or an end in themselves.

Compared to state institutions and government bodies, private companies are often easy prey – they will not have the same level of protection and may not be as mindful of the range and severity of the threat yet, still have much information worth taking, whether it is technical info which can be reverse-engineered, data which gives their own corporates a competitive edge, or just 'sensitive' information which could prove of use in the Great Game.

We recall a major energy company which, for at least six months, was unknowingly transmitting all of its experimental data to a foreign nation with designs to compete in the UK energy sector, or the electronics firm which resorted to erecting a *'Faraday cage'* around its most recent bid proposal, after all previous versions

A Decade of Intrigue

had been stolen by a nation with a competing firm (which was then able to undercut every time). Part of the issue is in not being aware that these attacks are even happening, such is the 'stealth' nature' of the cyber-attacks, and part is in not having adequate defences. It is by no means impossible to repel a state-sponsored attack, but such opponents will often have a great deal more power to bear so these defences must be top-notch.

Conclusions

As we look back on these past ten years a number of conclusions become immediately available. It is clear that despite claims to the contrary, an evolution is happening: in the way criminals conduct their business, in the tools that they use to do this, and in the degree of exactitude needed to combat these. What passed for security – in all its forms – even five years ago will not suffice now.

The one watchword we would offer is awareness. Be aware of the potential risks, weaknesses and threats associated with any new venture – and be aware that these will not be the same every time. Be aware that the issue of 'trust' is not one that can be easily solved by assuming the best or by believing what you see. Be aware that hacking into a computer is just a small part of the overall cyber-threat. And be aware of the big picture. What might seem innocent or unimportant now could have fatal consequences down the line.