

Play Up, Play Up, And Play The Great Game

18/09/2017

The drones of today can be applied to many purposes. Surveillance footage of a suspected terrorist hideout? Certainly. Delivery of online shopping purchases? If you like. Finding out whether the big game formation will be 4-4-2 again? Hang about...



At the 2014 World Cup in Brazil, headlines were briefly made when the French national team claimed that a drone had been spying on their training sessions to determine formation and tactics. While nothing was ever proven, the spectre of tech even more controversial than goal-line technology was reawoken last week when the English FA announced that, assuming qualification, players and staff heading to Russia would be subject to strict guidelines on Internet usage, to prevent giving any edge away to opponents who could be looking to hack their communications.

This is actually an extremely sensible idea, not least due to the location in the *'wild east'* of Russia, where data interference flows as frequently as vodka. The practice of hacking into wi-fi has long been established and has given rise to the *'pineapple'* phenomenon - whereby public areas such as coffee shops, airports and hotels have wi-fi that is easily compromised. Too often, free wi-fi is treated as a blessing rather than with the suspicion it richly deserves. Not for nothing are business travellers to locations such as China, Africa and, yes, Russia urged to never use it: the risk is simply too great. And while there may be data far more important than the England team line-up to be gotten through hacking wi-fi, in principle the FA's actions are entirely correct: if you have something that is valuable, even if that value has a time limit, do not take the chance.

The issue of drones spying on training sessions is perhaps a little more fanciful, but only just. After all, if drones can be used to track terrorist movements and actions, why not those of a football team? Whether true or not, it would hardly be the first instance of corruption in football at the, literal, grassroots level - not even counting the actions FIFA and its ilk. If the information is that valuable it is, the argument runs for some, expedient to do whatever you can to obtain it.

The wider lesson is this: whatever your business today, there are those that will do anything to gain a competitive advantage, and inventive new methods of what amounts to corporate espionage will constantly be applied. Already the social media revolution can speak volumes of what happens when too much

information is freely shared, and devices such as the pineapple that compromise everyday life without us even realising present new challenges for the security-conscious. We might not see drones flying around Wall Street or Silicon Valley to eavesdrop on each other with regularity, but in the worst case this is not beyond the bounds of possibility and in the best case, would just be a visible symptom of the espionage problem. From passively picking up anything said on an unsecure connection, to specifically planting a source inside a company to pick up intelligence, there has never been a time where corporate espionage has been more frequent, or the need to prevent it more vital.

The great game of corporate espionage is alive and well. As any football manager would tell you, getting the defence sorted is rule number one.

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@kcsgroup.com or call (00 44) 2072451191**
