KCS Group Europe

Chinese infiltration: espionage on the increase

July 2023

The threat from within is being ignored. The intelligence community has been issuing warnings for companies doing business with China for some years. However, the situation in recent months has become far more serious, with the theft of intellectual property reaching unprecedented levels.

The National Counter-intelligence and Security Centre (NCSC) recently warned of an update to China's counterespionage law, which came into effect on 1 July. This has the potential to create even greater risks and uncertainty for any company wanting to do business in China. The NCSC adds that the update broadens the scope of China's espionage law and expands Beijing's definition of espionage. Any documents, data, materials or items could be considered relevant to the law due to its 'ambiguity'.

The revisions have raised further concerns for Western companies, which already find themselves caught in the middle of an increasingly fraught relationship. But while China seeks to protect its own interests from the West, the corporate world in the UK and the EU blindly and naively believes that it is secure enough not to have any concerns or fears about external interference. In many instances, companies believe the threat is exaggerated.

Many Intelligence and Human Resources Departments are busy focusing on sanctioned Russians and those breaching sanctions, but paying no attention to the more subtle activities of the Chinese. The intelligence industry has always subscribed to the 'Thousand Grains of Sand' analogy – if intelligence were sand, the Russians would collect it in a digger, while the Chinese would collect a thousand grains – one at a time. This has never been truer.

Whether it is through sophisticated cyberattacks or discreet placement of key individuals operating under pretext, the level of penetration being achieved by the Chinese is significant. Unfortunately, Western corporations remain ignorant as to the depth the Chinese will go to achieve their objectives.

Businesses of all persuasions are potential targets for those seeking inside information. Companies such as those providing accounting and legal services are being targeted as they provide relatively easy access to more secure organisations in the defence and communications sectors. Both of these are areas of interest to the Chinese government. Too many organisations are suffering from commercial arrogance, ignorance and naivety. Taking press reports and stories with a pinch of salt means that they remain oblivious as to the level and depth of Chinese subterfuge.

Internal auditors and human resources are not equipped to deal with this type of threat and companies must do more – much more – if they are to protect themselves and their intellectual property from state-sponsored intrusion. More than ever before, applicants of all persuasions need to be thoroughly vetted and screened. Next time you consider employing an intern, a Chinese student – or indeed anyone for a permanent or temporary position – make sure that your research is thorough.

According to MI5, a number of students have had to leave the UK over the last few years because of the espionage threat posed by Beijing. According to the same agency, China is heavily targeting industrial secrets and intellectual property. No companies are immune. The FBI has warned that it is opening a new China-related cyber investigation every twelve hours. This represents a 1,300% increase over the last seven years. In the UK, MI5 has said that it is now conducting seven times as many China-related cyber investigations than it was in 2018.