



COMPETITIVE CROOKS

PAUL HAWKES

Just over six months ago, a property dealer decided to disregard his contract with a major property firm and misrepresent himself, which, undetected, could have netted him a multimillion pound fraudulent bonus. Fortunately, our clients were tipped off, and prudently decided to conduct a thorough and focused professional investigation.

Despite identifying numerous pieces of circumstantial evidence, all pointing at the probability of the fraud having taken place, it became clear that our suspect was actively and cleverly covering his tracks. This could have led to a possible lengthy and costly investigation. However, during the investigation, we came across a bundle of shredded paperwork that we knew had come from the office of the suspect. Out of 147 assorted documents partially and painstakingly put back together, a two-page letter emerged, described by my client's solicitors as 'the equivalent to a smoking gun'.

It's an interesting tale, but its significance in terms of intelligence security is that, while sifting through the reconstructed shred, I was struck by the depth of information we were privy to. Most of the information that was not directly relevant to the case was actually the highest quality corporate competitive intelligence and, if the reasons for wanting to acquire the information had been different, its loss could have revealed havoc. This underlined the fact that all intelligence tools and techniques may be used legitimately or illegitimately and, in my experience, hostile intelligence gathering is far more common than you would believe.

Current legislation – such as the Waste Reform and the wide-ranging and, some believe, tedious 1998 Data Protection Act – is designed to curtail the legitimate use of confidential information. The Data Protection Act was originally brought in to regulate the free flow of sensitive information, causing great concern and paranoia within the corporate legal world. The act has been written in such a way – one banker recently assured me – that carrying three business cards in

one's wallet, while not registered as a 'data controller' with the Data Protection Registrar, could well be interpreted, within the terms of the act, as being criminal.

The point is that in terms of practical protection against hostile intelligence gathering, the Data Protection Act offers very little. Over the last few years since the Act was written, in my role as a counter-intelligence consultant, I have come across numerous cases where clients' competitors have been proved to be aggressively gathering intelligence, in most cases with a degree of legality.

'THE FACT REMAINS THAT THERE ARE DEDICATED EXPERTS OUT THERE, WHOSE SOLE PROFESSIONAL PURPOSE IS SIMPLY TO BREACH YOUR SECURITY'

As corporate competition becomes increasingly fierce, legitimate investigative techniques that are traditionally aimed at proving fraudulent activity are increasingly being used as a weapon by some aggressive intelligence gatherers. Neither the Data Protection Act, nor other laws appear to have acted as a deterrent in these cases. I know of an anonymous affiliation of 'data miners' (data collectors), who are based in the US and protect themselves by using pseudo names and religious or military titles as a means of identifying themselves.

Members describe themselves as information mercenaries and will, for a fee, breach and access sensitive information, such as offshore or private-numbered accounts, and

printouts of calls made from telephone lines. I am also aware of set-ups in former Eastern Block countries, which offer bespoke viruses designed to breach standard firewalls, with a view to accessing data network information, including email.

The point is that however conscious or alert we are of the many security issues, and however protected we may feel by the various legislations, the fact remains that there are dedicated experts out there, whose sole professional purpose is simply to breach your security. I personally believe it is commercially healthy to take as much responsibility as is reasonably possible to both identify, everything your competitors would love to know about you, and to protect it.

The problem that besets all those that consider themselves experts in the field of information security is that the information mercenaries mentioned above are constantly changing and adapting, requiring information security experts to change, adapt, defend and protect to stay ahead.

Thankfully, in many cases, businesses now seem to be taking information and security threats more seriously. Many UK companies are following the US lead and appointing chief privacy officers, or retaining competitive intelligence consultants and other trusted professionals. Chief privacy officers typically take the responsibility of information security professionals a few steps further, constantly reviewing and challenging their own systems, respecting their competitors' capabilities and methods of competitive intelligence gathering, while remaining vigilant to any potential threat.

It is well worthwhile to remain alert to the threats to our systems because, wherever there is success, there are always those wanting their unfair share. ■

PAUL HAWKES is the senior partner of Research Associates and has practiced as a professional investigator and competitive intelligence consultant for over 25 years. paul.hawkes@investgator.com