

# THE SPECTATOR

## Is that a bug under your boardroom table?

**Dominic Midgley explores the increasingly respectable and lucrative profession of corporate espionage**

June 24, 2006  
By: Dominic Midgley

The news that Michael Howard, the former leader of the Conservative party, is to become the European chairman of Diligence, a US-based corporate intelligence company, is the latest sign of gentrification in a sector that was once seen as the preserve of shifty types who rifle through bins under cover of darkness.

There is still a role for that sort of operator, but as the commercial investigation game gets serious, a growing number of private investigators have a background in investment banking or the law. Indeed, one security industry analyst, Equitable Services, has predicted that the global private security market could be worth GBP 150 billion by 2010, fuelled by mushrooming demand for high-quality commercial intelligence.

As more and more billionaires emerge from the Middle East and Eastern Europe, for example, there is a corresponding need for forensic analysis of the source and stability of their wealth. And companies such as Kroll Associates, Control Risks, Risk Advisory, GPW and even Pinkertons, the venerable American private detective agency, are prospering as never before. Kroll alone is said to have a turnover of \$1 billion.

As the quarry becomes increasingly sophisticated, so the investigators are trading up. Diligence, the firm that Howard is joining, was founded in 2000 by a small group of ex-CIA and MI5 officers; it is chaired by Richard Burt, a former US ambassador to Germany. The careers page on its website provides a neat illustration of the way the corporate surveillance industry is going.

'While our staff include many people with extensive governmental and business backgrounds,' it says, 'we are actively recruiting young and mid-career professionals from intelligence, journalism, business and finance who want to build exciting careers in this burgeoning new space.' The employee featured on the home page is Nada Bouari, one of Diligence's project managers; a former investigator with the Volcker Commission, she specialises in fraud and compliance issues, and is fluent in French and Arabic.

Another good example of the professionalisation trend is Paul Austin, a former ad-man who is now a corporate intelligence consultant. 'Some of the low-rent companies will resort to anything to get information but we rely on a network of contacts and creative business thinking,' he says. 'I'm certainly more likely to be found at the bar of White's having a sneaky G&T with a contact than I am to be rummaging through someone's bin.' The role of the modern private dick can range from

running the rule over a company that is being targeted for takeover to tracing damaging internal leaks. 'Essentially, corporate intelligence is about getting the upper hand in business,' says Austin. 'The real skill lies in extracting information from people without them knowing it, or simply in going through hundreds of pages of figures until you spot something which is a bit dodgy.' A typical operation will involve a public records search, a Companies House search, a shareholders' search, and even a Land Registry search to establish property ownership, in addition to a thorough review of the target's asset base.

More informal inquiries are conducted by contacting former colleagues of key players and people with whom they have been in litigation. Austin adds: 'Surveillance is a large part of corporate espionage. There's not usually a problem if the chief executive is bonking his secretary, but there is if he's drinking a bottle of vodka a day. That's the type of thing that you can find out through surveillance.' In situations where business intelligence can pay rich rewards, there is a temptation to play fast and loose with the law by paying for phone and bank records. Such practices are not endorsed by reputable companies such as Diligence and Kroll but a number of smaller outfits do take advantage of them. In a Guardian article on the murkier side of information gathering three years ago, the respected investigative journalist Mark Hollingsworth wrote, 'There are only between five and ten people in the country who can directly access bank and telephone records and they are treated like royalty in the industry.' 'When you go to see them, it is a bit like buying heroin from a dealer or meeting a Hollywood superstar,' one operative told him.

'You have to handle them with care. They will deliberately keep you waiting as if they were a tycoon. But some of them don't know their financial value, because you can get decent information off them for GBP 200 and then sell it for GBP 1,000.' Aside from bribing employees of telecoms companies and internet service providers, the more unscrupulous will also resort to bugging. It's hard to gauge how widespread such a practice is: no one wants to go to jail for being caught red-handed installing a recording device, but the long list of bugs advertised for sale in magazines such as Exchange and Mart indicates a growing market for them.

And a number of companies, normally staffed by former policemen or soldiers, are certainly making a good living by feeding off corporate paranoia. 'Companies often have sweeps done as part of their routine during takeovers,' says one. 'Or they contact us because of information having leaked. If the client believes there is a threat, we would ask them what made them think they might have been targeted. They might have launched something novel only to find that a competitor seems to be in line with them. The question then is: are they just good or has something been leaked?' The sources of such leaks fall into two main categories: human and electronic. The human factor could be a disgruntled employee, a cleaner or even a security guard categories of worker who have access to offices after hours, when there is most scope for rummaging through drawers unobserved.

Security experts recommend that all such employees are screened, but if the leaker is already in place the only solution is to mount an investigation. When one large blue-chip discovered that a national newspaper had planted someone in the company and that the individual concerned was passing on highly sensitive and embarrassing information, it hired a team of private investigators.

'They found the mole by going through the company's mobile phone records and emails, and by lots of surveillance,' says one source.

'They ended up putting a tracker on his car which showed him driving to the headquarters of the newspaper, and they got him.' Such witch-hunts can have tragic consequences, however. Abbey once called in Kroll to identify the author of an anonymous document that alleged a scandal over

bank contracts involving ex and corruption. The consultants from Kroll duly set about dredging through computer records and interviewing staff members. They obviously found their man. Shortly after being grilled by the investigators, an Abbey employee called Richard Chang, aged 48, jumped out of a fifth-floor window.

Electronic threats, meanwhile, vary from bugs to key-loggers, which record keystrokes on computer keyboards and can be used to collect copy or passwords. Bugs come in all sorts of shapes and sizes, from tiny battery-operated QPDs (Quick Plant Devices) with a battery life of 12 to 36 hours, to bulkier mains-powered affairs. QPDs are so small and cheap that they can be dropped into wastepaper baskets, with no need to retrieve them after their eavesdropping has been completed.

It was presumably a QPD that was responsible for bugging the Manchester United changing-room last November. The Sun was offered tapes of pre-match and half-time team talks, plus the celebrations of jubilant players after coming off the pitch, having successfully ended Chelsea's run of 40 matches unbeaten. On the tapes according to the Sun Sir Alex Ferguson could be heard exhorting his players and giving tactical tips to Wayne Rooney.

Targets of eavesdroppers are not entirely defenceless, however. Bugs can be traced using gadgets such as radio receivers that tune into the bug's transmitting frequency and there is even a new generation of what might be called electronic metal detectors.

But there is no real substitute for the old-fashioned approach. 'In the search for bugs, physical searches are very important,' says one consultant. 'Ceiling voids are very spacious.' If your company looks ripe for a takeover, you would be wise to keep a torch and a ladder in the boardroom.