

# Corporate espionage is entering a new era

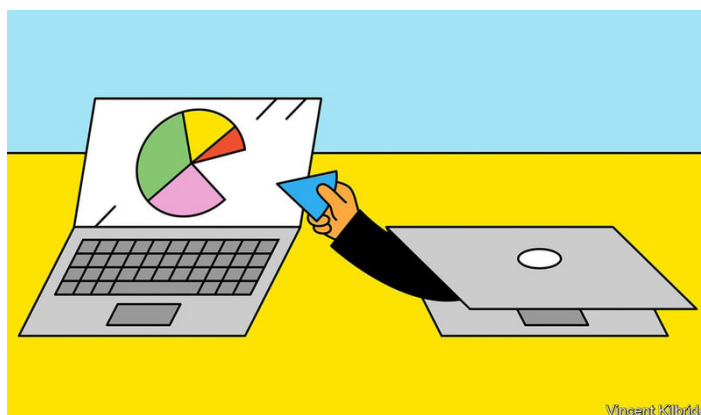
Companies need to take it more seriously

FOR ESPIONAGE of the cloak-and-dagger variety, it is hard to beat John le Carré or Ian Fleming. But the world of corporate spying has plenty of drama, too. Take the alleged skulduggery in a recent court case involving two American software firms. In May a jury awarded Appian, based in Virginia, \$2bn in damages after it had accused Pegasystems, from Massachusetts, of illegally snooping on it to gain a competitive edge. The trial revealed that Pegasystems executives had referred to a contractor hired to obtain ingredients of Appian's secret sauce as "our spy" in internal documents, and had dubbed the overall effort "Project Crush". Pegasystems, whose share price slumped after the ruling, and which is set to face a barrage of class-action suits from disgruntled investors, has vowed to appeal against the "unjust" decision.

There are two intertwined reasons for this: the inexorable growth of the intangible economy and the growing sophistication of online hackers. CEOs should be worried when they see their firms' secrets being hawked on the dark web; one marketplace, Industrial Spy, flogs stolen data and documents to "legitimate" businesses. Information is sold in packets ranging from a few dollars to millions. Keeping intellectual property (ip) safely locked in the digital vault can be devilishly difficult.

When they hear about ip, most people think of patents. Securing patents has become more difficult, in America at least, since a pair of Supreme Court rulings in the past decade chipped away at, respectively, protection for "business methods" and "abstract ideas" (which many software-based inventions are). This has left companies more reliant on developing and safeguarding trade secrets. These can be anything from algorithms and client lists to chemical processes and marketing plans. Among the most famous trade secrets are Coca-Cola's recipe and the formulation for wd-40. Most are more mundane: recent legal battles have involved industrial-baking agents and floor-resin formulas. Patents offer stronger protections, but trade secrets last for ever—if they are well kept.

Christine Streatfeild of Baker McKenzie, a law firm, talks of a "pivot" in the past five years, as more companies in more industries wake up to the need to protect their secrets. She points to stepped-up efforts in consumer goods, steel



and even cannabis. Baker McKenzie has advised legal marijuana-growers in America on steps they can take to curb rivals' access to information about their cultivation techniques, soil recipes, extract flavouring and so on.

Digitisation makes the problem thornier. As old industries, from carmaking to education, increase investment in software, they have more bits and bytes worth stealing. Industries with lots of startups are particularly vulnerable, says Sidhardha Kamaraju of Pryor Cashman, another law firm, because they combine lots of new tech with mobile employees who hop between up-and-coming firms. In 2018 Alphabet's Waymo self-driving unit won a \$245m settlement from Uber after alleging that one of Waymo's former engineers took trade secrets along with his office bric-a-brac when he left for the ride-hailing firm.

At least legislative protections for trade secrets have grown stronger. A turning point in America was the Defend Trade Secrets Act, passed in 2016, which greatly expanded the type and number of secrets covered by federal law. Its passage led to a 30% jump in cases filed, says Tim Londergan of Tangibly, an ip-management firm.

The bad news is that many firms are poor managers of such secrets. It is not enough to make reasonable efforts to keep the information confidential. The secret also has to be clearly articulated. Failure to do this has been exposed in a number of recent cases. In one, Mallet, a baking-products firm, failed to block an upstart rival from using release agents (which allow loaves and buns to be more easily removed from pans) similar to its own, after an

American appeals court ruled, in effect, that Mallet hadn't adequately described and documented its secret formula.

Such rulings have led more bosses to demand "ip audits" and use the results to better safeguard secrets. This, in turn, has spawned a cottage industry of trade-secrets consultants. Lawyers, too, are in demand. Patent lawyers are plentiful but few really understand trade secrets and they tend to focus on litigation, once the problem has arisen, says Mr Londergan. "Companies need help earlier." They also need to focus more on risks emanating from corporate partners, for instance in joint ventures. This is often an afterthought even among multinationals.

## Corporate Bonds

TSMC is a rare globally active company that comes close to best practice in articulating and managing its trade secrets. The Taiwanese chipmaker has good reason to want to get it right. It operates in a highly sensitive industry chock-full of proprietary information that rivals would love to get hold of. On its doorstep is China, which bears Taiwan ill will and is widely acknowledged as the world leader in ip theft (having been its victim in the 18th century, when Jesuit priests were sent from Europe to nick Chinese trade secrets in porcelain-making). The Taiwanese authorities say that in recent months they have uncovered several attempts by China to poach semiconductor engineers using Chinese firms that registered on the island unlawfully by hiding their origins. In May Taiwan's parliament passed a law that punishes anyone who obtains or uses designated "core" technologies for the benefit of "external entities" with up to 12 years in prison.

America, too, has cracked down with China in mind. The Department of Justice says that roughly four in five economic-spying cases it brings "allege conduct that would benefit the Chinese state". The best-known case of suspected espionage by China, involving Huawei, a maker of telecoms gear, is the tip of a large iceberg.

As big a threat as China is, it isn't alone. Ostensibly friendly states spy, too. Israel has been known to snoop on American firms for the benefit of its tech and military industries. And it is not always helpful to think of the threats posed by different kinds of actors—company insiders, corporate rivals or governments—as discrete. Sometimes they are at work simultaneously. Take the recent sentencing of You Xiaorong, a former chemist at Coca-Cola, to 14 years at Uncle Sam's pleasure. Ms You was convicted of stealing trade secrets relating to coatings on the inside of beverage cans. She used the filched formula to set up her own company in China, with backing from a local partner. Their venture received grants from the

Chinese government. Whether or not Chinese officials were aware of the theft is unclear.

The case highlights another challenge for firms trying to keep a lid on secrets. They can spend as much as they like on beefing up it systems, but they must still watch out for analogue forms of exfiltration. Operatives for Procter & Gamble (p&g) were once caught diving in dumpsters outside a Unilever office in Chicago in search of information about its consumer-goods rival's marketing strategy. Ms You apparently used her phone to take pictures of sensitive documents to bypass Coke's security measures. People use smartphones in offices all the time. How to tell if it is for nefarious reasons?

Moreover, much corporate spying can be—from the point of view of those being spied on—frustratingly fuzzy. Some of it is perfectly legal. Many hedge funds watch activity in factories, using foot-soldiers or satellite imagery, to gauge output and bet accordingly on stocks. At the other extreme is stuff that no ceo in their right mind would countenance: p&g's top brass were so appalled when they learned of their underlings' trash-rummaging at Unilever that they shopped their own company, resulting in a \$10m settlement.

In between is a large grey area where operatives "ride the ragged edge" of morality and the law, as Eamon Javers puts it in his book, "Broker, Trader, Lawyer, Spy". Many of them work for outfits that companies hire in order to gain plausible deniability. This industry came of age in the vicious takeover battles of the 1980s and has since grown at breakneck speed. Its well-known names, such as Kroll and Control Risks, are at the top of a pyramid containing thousands of mostly small firms.

Most such work is legal and boring—for instance, due diligence on clients' prospective business partners. But there are cases of firms undertaking dubious activity, from wiretapping to impersonation. In the 19th century, the industry's grandfather, Allan Pinkerton, laid out (and largely followed) a strict code of conduct. Mr Javers fears that some of Pinkerton's modern-day counterparts routinely violate many of his gentlemanly commandments.

None of this is going away. Employee mobility is at or near an all-time high. Companies, and the tactics they use, get more desperate in downturns. And the geopolitical backdrop is growing frostier, increasing incentives for underhand activity by states or their proxies. "Casino Royale" it may not be, but the spectre of surging economic espionage is real.