Back in fashion — trade secrets in the modern enterprise

With increasing uncertainty in the patent landscape, trade secret protection is becoming more important for businesses than ever before

By **James Pooley**

If you have strategic responsibility for intellectual property, then you may already feel the ground shifting beneath you. Patents have held sway during our professional lifetimes not only as a marker of innovation, but as the main way in which companies protect and exploit their competitive advantage. Not any more. Like an old style of dress, trade secrets are coming back into fashion and turning heads.

This new focus on secrecy may be distressing to the few who deny that trade secrets even deserve to be classified as intellectual property. However, they are in fact the oldest form of intellectual property, rooted more in self-help than in sophisticated legal frameworks and covering much more information than just inventive technology. Perhaps the most striking difference between trade secrets and other forms of IP rights — apart from the lack of any government certification — is that secrecy is not an exclusive right, but protects only against theft or misuse in a confidential relationship. So keeping business secrets requires a great deal of care and attention.

Secrecy itself is certainly getting attention these days, ranging from news stories of audacious hacking to hand-wringing about the diminishing clout of patents to political attempts — most notably a proposed EU directive — to provide a more harmonised environment in which businesses can assert their trade secret rights.

However, just because secrecy is newly popular does not mean that it is simple to use. Indeed, today's hyper-connected, globalised economy makes it more challenging to work with this form of intellectual property. Yet thoughtful trade secret management can bring big returns and avoid big problems. Here are seven critical issues to consider.

To share nor not to share?

It is a cliché of the information age that intangibles have replaced hard assets as the foundation of industry. This shift has happened with astonishing speed. According to Brookings Institute studies, in 1978 80% of the value of publicly traded companies was associated with tangible property. Within 10 years this had dropped to 45% and by 1998 the ratio was 30% tangible to 70% intangible.

Looking at how this intangible property is protected, secrecy is definitely on the rise. Of course, it has always been a favoured method for process technology, where patent infringement would be difficult to detect. All patents start out as trade secrets, since most of the world lacks a grace period and insists on absolute novelty. However, shorter product lifecycles in fast-moving markets have made patents less valuable in many sectors of the economy. A Carnegie Mellon survey of US R&D firms reported in 2000 that secrecy was used more than patenting to protect innovative results. This trend was confirmed in 2009 by a study by the National Science Foundation and the Census Bureau, which found that for companies classified as R&D intensive, secrecy was chosen more than twice as often as patenting.

And yet these increasingly valuable trade secrets have never seemed more vulnerable. Cyberattacks are relentlessly successful. The same communications technology that has enabled extraordinary advances in global productivity seems to have made

information loss almost inevitable. And it is not just the Internet, but also mobile devices — such as USB drives and smartphones — that imperil data security. Many business executives are now forced to strip their laptops clean before and after travelling.

It must therefore seem perplexing to business leaders when they are told that proper exploitation of information assets requires that they be shared broadly, sometimes with companies located in countries without strong IP protection. This is the sharing dilemma and it is a recent phenomenon. A century ago, Henry Ford established a new paradigm for industry with vertical integration — from its own rubber plantations to its own foundries to its own transportation networks, Ford controlled every aspect of the design, production and distribution of its vehicles.

However, as the world shrank, the realities of comparative advantage forced business to begin outsourcing some important functions. The information economy accelerated this trend and gave birth to open innovation, in which companies reach outside for product ideas and engineering solutions. In fact, one of today's most enthusiastic proponents of this process is the Ford Motor Company.

Open innovation is not the same as open source, in the sense that it can be practised by a small number of actors working under a specific agreement. However, it does imply the need to share information, because the best collaboration will result from each party knowing the other's product platform and direction, in order to be able to add value from its own special perspective or technical assets. Scale this up to many simultaneous transactions, driven largely by global supply chains, and you have the modern enterprise: fully dependent on creating and controlling information as an asset, but also on distributing that information into a network of temporary and often shallow relationships.

Living with this dilemma requires careful management, particularly in cross-border deals. Circumstances vary, but here are a few tips for reining in the risks:

- Choose your partners carefully. Are their concerns about information security aligned with yours?
- Recognise that secrecy laws — and particularly enforcement mechanisms — vary significantly, despite the promise of harmonisation through the Agreement on Trade-Related Aspects of Intellectual Property.
- Understand not only local laws, but also local customs that might affect the behaviour of trusted individuals.
- Do not rely on the time-worn principle of using the same level of care as for your own information. Instead, specify exactly what you expect your partner to do, particularly with its own employees and consultants.
- Demand inspection and audit rights for information security.
- Agree on effective enforcement, for example in your home jurisdiction, or by arbitration (with discovery, so that you can access the facts).

Cyber threats

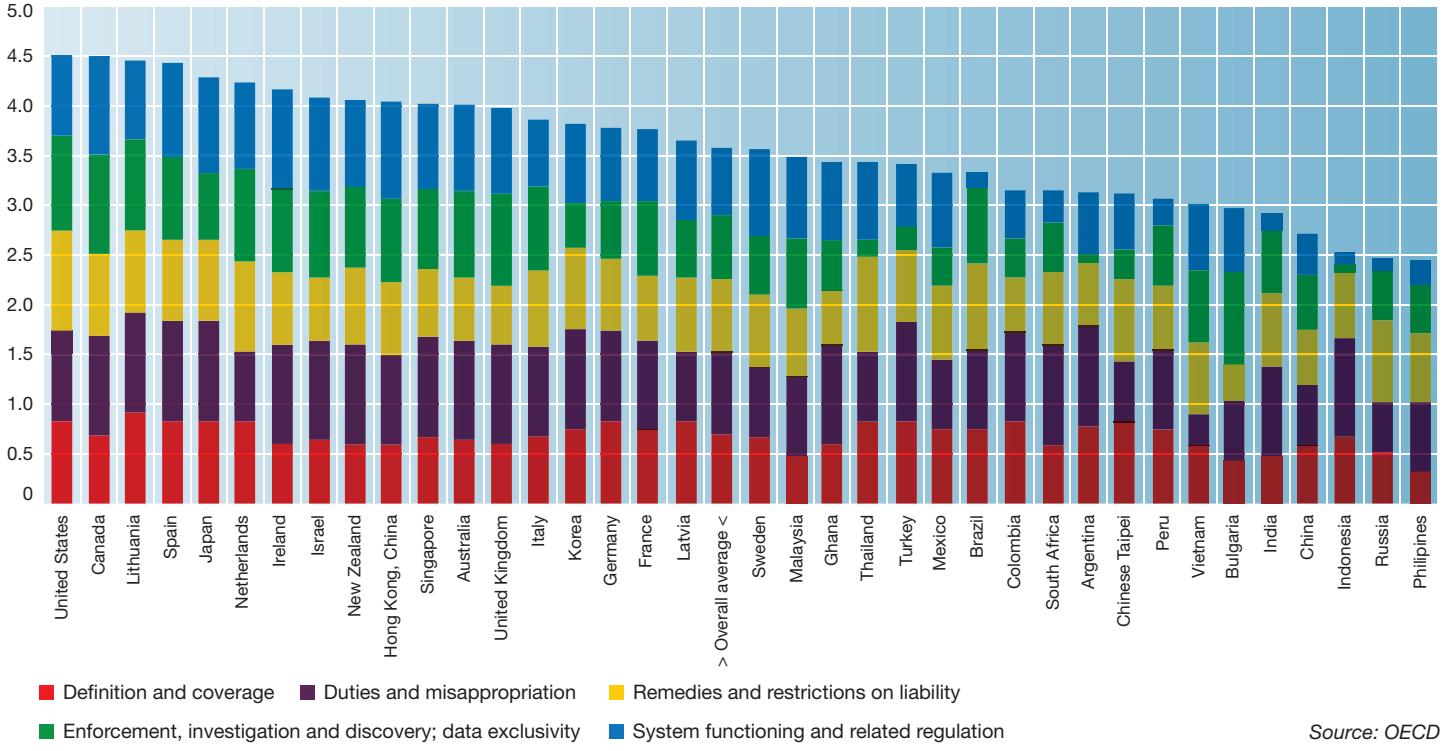
When I first worked with clients on trade secret issues in the 1970s, information security was straightforward: watch the photocopier and watch who went in and out of the building. Things became more complicated with internal computer networks, but IT personnel and systems controlled and recorded every access point. Once corporate systems were connected outside, and particularly with the advent of the Internet, everything changed. Making all data available anywhere in the world 24/7 was not just a desirable feature, but an absolute requirement for doing business. Protecting the perimeter of the information castle grew increasingly difficult.

Perhaps we should have anticipated this. With information becoming a kind of currency, hackers acted like bank robbers and went to where the data was. Sometimes it was just to cause damage, as in denial of service attacks designed to overwhelm a company's servers. But with increasing sophistication, cyberthieves have repeatedly penetrated the perimeter, planting malware that anti-virus software cannot recognise and taking time to discover, collect and quietly send out a company's most valuable information.

The image of handling security by watching the front door now seems impossibly quaint. Because commercial networks are connected to thousands of laptops, tablets and smartphones (many of them belonging to individual employees), there are now practically uncountable doors leading into a company's information vault. The coming Internet of Things, with fully connected locking systems, printers and videoconference equipment, will only make the problem worse. A recent review of internet-connected commercial devices found that between 40 million and 50 million of them were using old protocols with known vulnerabilities.

As a result of this new dynamic, most security professionals take the view that defending the perimeter alone is a fool's errand, and that a smart strategy assumes that a number of barbarians are already

Figure 1. **Trade secret protection index, by economy and component, 2010**



Source: OECD

inside the gates. As a result, the focus is on detection and response, to affect the consequences of breaches rather than assuming that these can be prevented.

However, managing risk in this environment is not only about your own IT systems. Because every company is connected to one degree or another with a variety of vendors, customers and collaboration partners, many of which have trusted access, a company's risk profile extends to all of those third parties. Their security readiness becomes your own. Recall that the Target breach did not happen by a direct intrusion of its own system. Instead, access was accomplished through its air conditioning contractor, which had less sophisticated protections in place.

The lesson here is that proper management of information assets against cyberattack requires much more than hardened IT defences. It must be seen as part of a comprehensive and cross-functional assessment of risks and priorities.

Insider threats

One information security risk that has not really changed in decades is the careless behaviour of insiders. While we all make mistakes, studies show that it is employee forgetfulness and lapses in judgement, rather than deliberate espionage, which cause the greatest amount of information loss.

This is not just about the rank and file. It was an executive at Nortel, absentmindedly clicking on an attachment to what appeared as a normal email message, who began a silent, stealthy occupation of the company's IT systems which lasted most of a decade and ended up contributing to its downfall. (Security firm Websense has calculated that two-thirds of these phishing emails are sent on Mondays and Fridays, when people are presumed to be more hurried and less careful.)

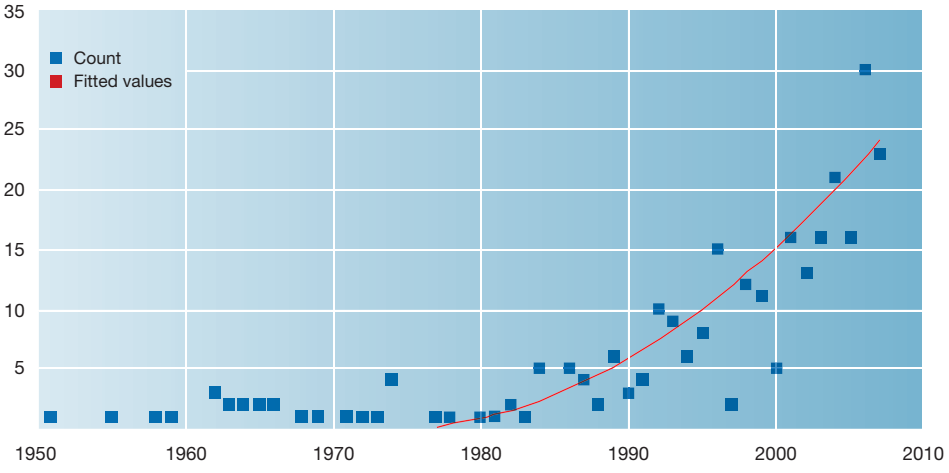
At least two aspects of the insider threat have become more challenging for information security in recent years. The first of these is the more or less constant electronic connection between staff and the company. Employees work at home and on the road, often using their own smartphones or other mobile devices to stay in touch and get work done. This proliferation of personal equipment, dubbed 'bring your own device', reflects the fact that most corporate IT departments have surrendered in the struggle for absolute control of data systems. It was not so long ago that the BlackBerry, secure and

centrally managed, was standard issue for most employees. Now IT departments must contend with a potpourri of gadgets with various levels of security, requiring extremely sophisticated device management software to mitigate the increased risk.

The second shift has been in the attitude of the employees who are trusted to deal with the company's most precious and vulnerable assets on a daily basis. In particular, the millennials — otherwise known as the Facebook generation — have become accustomed to sharing information as a natural and desirable behaviour. Workers who spend their evenings in what may seem extreme acts of self-disclosure on social media are unlikely suddenly to change their habits when they log into a company's system in the morning. And they are more likely to engage in bad security hygiene — for example, by using public WiFi at an airport or hotel to check their company email, unaware that someone has planted a cheap man-in-the-middle device to tap their stream of data, looking for likely passwords or the opportunity to plant malware which can later infect the enterprise.

The good news about the insider threat is that there is a clear and cost-effective way to confront it: thoughtful, comprehensive policies coupled with effective training. Information security too often comes up only at orientation. Modern threats and responsibilities require a continuous programme of professional, varied (so it is interesting and memorable) and customised education about the employee's role in protecting the company's intangible property. These efforts should be constantly measured and evaluated to ensure not only that the message is being received, but also that it translates to everyday behaviour. Indeed, if this aspect of management is done correctly, staff will begin to understand the existential stake they have: protecting trade secrets protects their jobs.

Figure 2. **Decisions by year**



Source: "A Statistical Analysis of Trade Secret Litigation in Federal Courts", Gonzaga Law Review, *2010*

Inbound threats

One of the most profound shifts in trade secret management has affected the direction of perceived threats. It used to be that caring for your secrets meant keeping them inside the organisation or under strict control if they had to go outside. The outbound threat remains of primary importance, but now there is broad recognition that information integrity also requires vigilance against infection by unwanted data coming into the organisation.

As the word 'infection' suggests, it may help to think of unwanted information as a virus, with various vectors creating the exposure and with all the challenges of rooting out something that can morph as it self-replicates inside its new host.

The most common vector of infection is, unsurprisingly, new employees. Depending on the industry and nature of the job, new hires may believe that they can increase their chances of success by bringing helpful information from their former work. Then there are those (software engineers come to mind) who find it emotionally difficult to part with any of their previous work product. Naturally, this phenomenon is not new. However, its incidence has been increased by the ease of transferring large amounts of data, its detection has been made easier by technology and its consequences have become more serious in part by the imposition of criminal penalties. We should take a closer look at each of these factors in order to better appreciate the nature of the risk.

Taking information to a new job used to entail hauling boxes, or at least multiple physical folders, containing confidential memoranda, drawings or strategic plans. Depending on how much time the departing employee had available, these sensitive papers might be culled while assembling the package, or perhaps later, leaving no trace of their ever having been taken. Even in the early days of electronic media, storage actually cost something, so people were more likely to make thoughtful decisions about what to take. Now, with virtually unlimited memory capacity, employees default to save everything and, when leaving in a hurry, may default to take everything, if they can.

Certainly, the taking has become much easier, particularly if the former employer does not have sophisticated tools to detect copying or downloading behaviour. With a few keystrokes in a few minutes, employees can copy thousands of documents to a USB drive or send them as email attachments to their homes. Doing this all at once may raise suspicions, but often this cache is built up over time and its taking sets off no alarms. As a result, today's new hire, even with the best of intentions, may have swept up a great deal of sensitive data into his or her virtual briefcase.

Again, looking at how this used to happen, physical documents might sit in a garage for years without ever (apparently) being used. However, electronic records have a way of migrating to the next employer's platform where they can be more readily accessed by the new employee. And there they may sit, until a (perhaps unrelated) lawsuit is filed and modern forensic investigation tools uncover them. Thus, technology has made it more likely not only that this sort of behaviour will occur, but also that it will be discovered.

This leads us to the new consequences. In 1999, Boeing and Lockheed were in competition for an important defence procurement. Branch, a Lockheed employee, was hired away by a Boeing manager named Erskine. Branch brought with him a few proprietary Lockheed documents and, on discovering them, Boeing promptly reported what it had found. However, it turned out that Branch actually had taken over 25,000 pages of confidential information. Several years earlier the United States had adopted the Economic Espionage Act, for the first time making trade secret theft a federal crime. By the time the dust settled, Boeing had lost about $1 billion in rocket launch contracts, paid $615 million to settle civil claims and saw Branch and its former manager Erskine charged with federal crimes. As I describe below, this case has highlighted the compliance obligations faced by company management and directors.

Table 1. **Identity of alleged misappropriator**

	1950–2007	2008
Employee or former employee	52% (142)	59% (71)
Business partner	40% (109)	31% (37)
Unrelated third party	3% (8)	9% (10)
Other or unknown	7% (19)	5% (6)

Source: National Science Foundation/National Centre for Science and Engineering Statistics, Business R&D and Innovation Survey: 2008.

The inbound threat comes not only from new employees, but also (and increasingly) from part-time contractors and consultants. Because the relationships are short term, they carry less implied loyalty. And because contractors have often worked recently for competitors and consultants may be doing so concurrently, these relationships are also bristling with potential for infection, while the individuals struggle with the difficult mental gymnastics required to keep their known data properly categorised and walled off. Therefore, consultants need special management attention, particularly in the contracting process, where the dilemmas of concurrent loyalties and compartmentalisation must be confronted and dealt with. At a minimum, it must be established that obligations to others will be respected and the consultant's work will not be influenced by anyone else's trade secrets.

Another critical area for controlling inbound risk lies in the so-called 'make versus buy' conundrum, which relates to the trend towards outsourcing or open innovation. In its most common form, the problem arises when a company decides to enter a new market or sell a new product, but is uncertain whether this should be done through internal development or by acquiring the necessary technology. In the ideal situation, the team that inspects and analyses the acquisition opportunity should be separated from those who will be working on the internal project. However, frequently key technical personnel are common to both teams and are subject to the non-disclosure obligations which typically attend any inspection and assessment of the potential licence. So if the decision is then made to make rather than buy, the company faces a potential claim that its exposure to the external technology will have improperly influenced its internal development. As a description of the problem suggests, avoiding it almost always requires a complete and well-managed separation of teams, perhaps even using an independent company to perform the analysis.

Governance problems

When trade secrets were just an arcane facet of intellectual property left to lawyers and the IT department, there was no cause for concern at the board level, unless there was some significant litigation. Now that secrets can constitute the lion's share of a company's asset base, all of management, including the board, needs to be engaged.

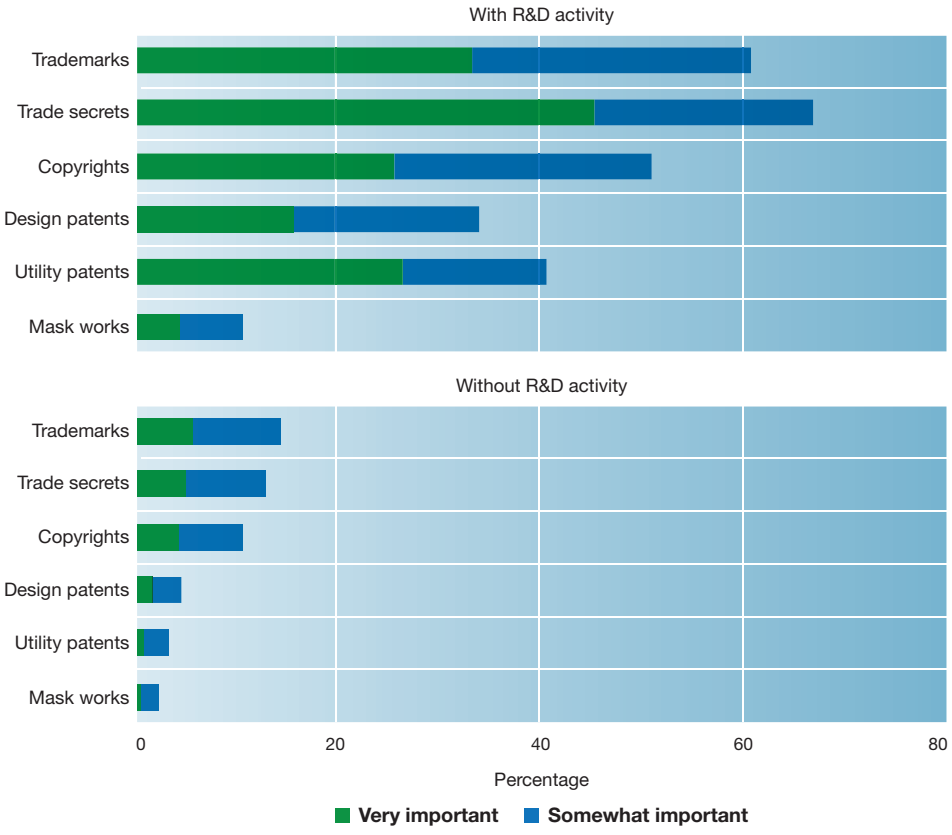
Avoiding liability is perhaps the most obvious reason to pay attention. At a fundamental level, boards and upper

management have a fiduciary duty to the organisation to ensure compliance with applicable laws. And as we have seen with the Boeing case, the consequences can be shattering. What should companies do to address this issue?

Criminal exposure to the Economic Espionage Act can be substantially reduced by implementing a compliance plan which meets the requirements of the Federal Sentencing Guidelines. Referring to criminal sentencing may seem a strange way to mitigate liability, but in fact the same guidelines used by judges to assess culpability at sentencing are also used by prosecutors to decide whether to seek an indictment in the first instance. This makes sense, because implementing a good compliance plan generally demonstrates that the corporation has done what it can to police its ranks and should not be called to account for the actions of one or two rogue employees. Here is a distillation of the requirements (note the emphasis on involvement of high-level management):

- policies and internal controls to reduce the risk of inbound contamination;
- board and senior management knowledge of the programme, with programme manager having direct access to the board;
- relevant training for the board and senior management;
- auditing and monitoring systems;
- incentives for compliance, discipline for violations; and
- prompt response to evidence of misconduct.

Figure 3. **Businesses reporting IP rights as very or somewhat important, by presence of R&D activity and type of IP right 2008**



Source: National Science Foundation/National Centre for Science and Engineering Statistics, Business R&D and Innovation Survey 2008

Although a compliance plan that qualifies under the Economic Espionage Act has no direct bearing on corporate exposure under the criminal laws of other countries, the principles should apply anywhere that the authorities are willing to consider preventive action by the company as a reason not to prosecute.

Boards have other reasons to be concerned about their responsibilities to protect and exploit the company's trade secrets. In the United States, a number of government agencies have recently shown an interest in this issue. For example, the Federal Trade Commission sued Wyndham Hotels in 2012 over a hack of its computer system which exposed customer information and caused $10 million in fraud losses. The basis for the charge was that Wyndham's management had "faile[d] to maintain reasonable security" for its network; the Federal Trade Commission claimed that this violated laws against unfair and deceptive behaviour. A recent decision of the Third Circuit Court of Appeals affirmed that such claims are within the agency's mandate. A related shareholder suit was dismissed only because Wyndham took prompt action to review and address its vulnerabilities. Even though this case was about personal privacy information, it is not hard to imagine the same analysis being applied more generally to neglect of critical security issues.

In 2011 the US Securities and Exchange Commission issued guidelines for cybersecurity which, although voluntary, are expected by many to become mandatory for listed companies. In 2013 the European Commission published proposed legislation which would require businesses to evaluate and address their information security risks, observing dryly that "industry should reflect on ways to make CEOs and Boards more accountable for ensuring cybersecurity". And in February 2014 the National Institute of Standards and Technology, an agency within

the US Department of Commerce, released its Cybersecurity Framework, describing best practices for the protection of critical infrastructure. However, the framework is written in a way that can apply to virtually all enterprises and security experts believe that it may become a *de facto* standard for prudent risk management of secret information.

Indeed, I believe that the National Institute of Standards and Technology's Cybersecurity Framework is a reliable starting point for any organisation trying to address information governance. Its guidelines are expressed in terms of classical risk management, making it easier to integrate information security into other corporate functions. Despite the word 'cybersecurity' in its title, the document covers the broadest aspects of protecting data integrity in an accessible way, describing separate levels of controls according to their complexity and cost (in terms of transactional overhead as well as expense). An Intel manager recently reported that using the framework helped to "harmonise our risk management technologies and language, improve our visibility into Intel's risk landscape, inform risk tolerance discussions across our company and enhance our ability to set security priorities, develop budgets and deploy security solutions".

Start-up risk

All of the information security risks faced by any company are multiplied and amplified in start-ups. In part, this is because of their heavy dependence on information assets — algorithms, business models, a novel product — to define themselves and justify heavy investment in their future. In part, it is because typical fledgling enterprises pay so little attention to security, focused as they are on just getting the prototype finished and completing the next round of funding. And while these risks merit more concern from founders, not to mention investors, there is one trade secret hazard that clearly stands out from the others: hiring.

As discussed earlier, all companies face the risk of inbound contamination when bringing on a new member of staff. However, for established organisations, this typically happens one person at a time and under circumstances that allow for sensible mitigation tactics: written assurances, careful onboarding with explicit warnings and specific orientation. Moreover, in larger firms it is easier to place someone in an area that will use their skills, but not necessarily appear to invite them to use confidential information belonging to their former employer.

In contrast, early-stage enterprises hire frequently and aggressively, often looking for proven talent from specific companies working at the cutting edge of development in their own industry. In other words, while in a race to get themselves established, they are hiring from the competition. They often have not had time to think about, much less implement, comprehensive procedures to address these issues. As a result, start-ups and their enthusiastic new recruits are more likely to make costly mistakes, casually passing on information which could be helpful to the new and growing team, but which should have stayed where it came from.

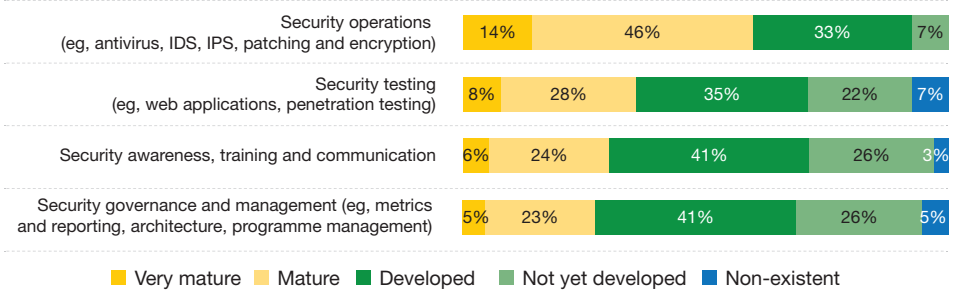
Even worse, this risky behaviour happens at a time when the enterprise is by definition more vulnerable to the costs and distraction of trade secret litigation, both of which can be devastating. This vulnerability is well understood by some affected competitors, which may be smarting from the loss of valued staff and looking for explanations other than their own mismanagement. With their incentives aligned this way, jilted former employers will frequently file lawsuits. Whether their primary motivation is to defend their intellectual property or to snuff out an incipient competitor by dragging it through a legal process will never be known.

Growing young companies (and those who support them) need to appreciate the special risks that they face in dealing with others' trade secret rights. It is not difficult to establish a programme that will work to reduce those risks while still allowing them to recruit the best and brightest.

Non-disclosure challenges

Especially with the new business focus on collaborations, non-disclosure agreements (NDAs) have become as common as PowerPoint decks. Many large companies cannot reliably tell you how many NDAs

Figure 4. **Maturity of information security management processes in surveyed organisations**



Source: EY Global Information Security Survey 2013

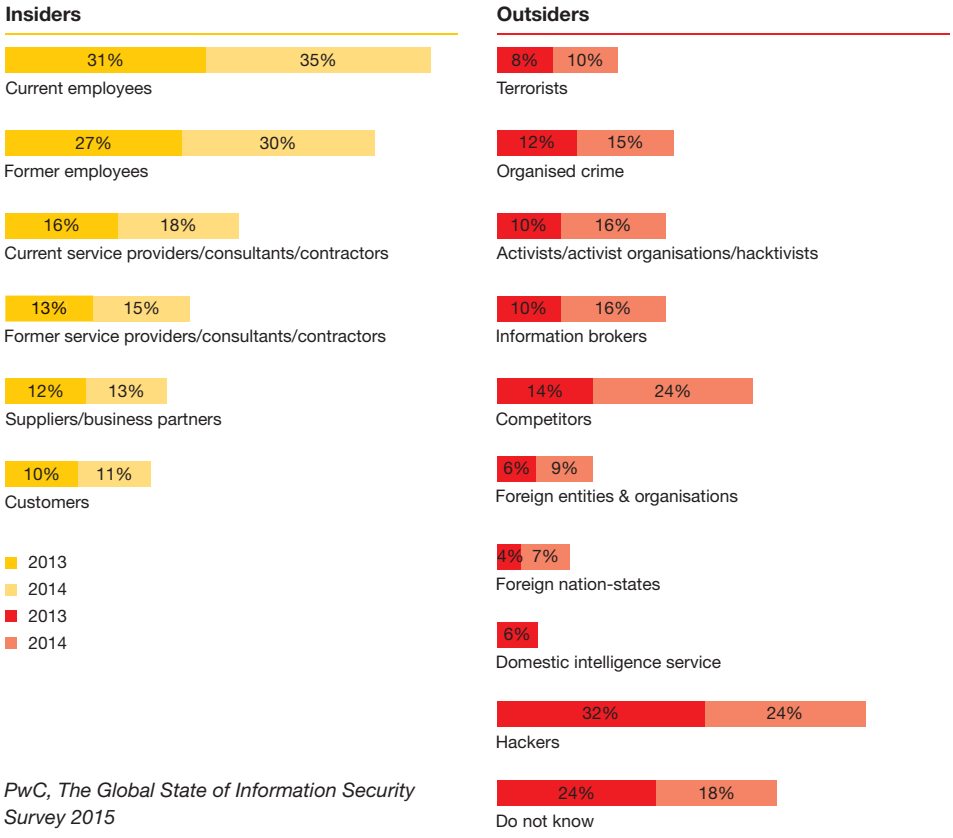
they have entered into. They certainly cannot tell you who is responsible for managing each one, exactly what the agreements say and whether they are all being complied with. It is ironic that as industry has come to depend so heavily on secrecy to protect its competitive advantage, its contracts are managed so casually.

The first shift of attitude must come in establishing NDAs: they are consequential agreements, not forms to fill in. They should be negotiated with an understanding of the specific benefits and burdens for each side, informed by candid discussion of what it is that the NDA is supposed to accomplish. That said, one should be careful not to negotiate the ultimate transaction at this stage. The NDA is a step on the path to the deal, not the deal, and the two should be separated.

The following terms should get particular attention in negotiations:

- Protection requirements — be sceptical of the standard promise to protect the other side's information with the same level of care applied to the recipient's. That level as applied to your information may be insufficient, so take the time to be clear about exactly how you want your data to be protected from inappropriate disclosure or use.
- Confirming oral disclosures in writing — be sure to protect yourself against future surprises by requiring that all oral disclosures of confidential information be confirmed in writing within a specific period. However, as noted below, be sure that you are ready to comply with this provision.
- Dealing with the residuals clause — some companies are unwilling to take confidential disclosures without what amounts to a partial waiver of your rights: there will be no protection for whatever their people might recall, as long as they do not refer to specific documents. The proposal should provoke a discussion of the concerns that prompted it, looking for an alternative. If that is not possible, focus on ways to limit its effect.
- Time limitations — consider controlling the back-end risk of a perpetual promise of confidentiality by limiting it to a term of years. However, keep in mind that this cuts both ways and sharing your own secret data on such terms may be tantamount to its agreed destruction.
- Export controls — do not forget that secret information may be subject to controls even when not transferred outside the country, if revealed to a foreign national.

Figure 5. **Sources of security incidents, 2013-2014**



PwC, The Global State of Information Security Survey 2015

The second change in perspective is about management of NDA obligations. Most of these agreements operate in both directions, so you may have concerns about how your own information is being protected by someone else, as well as how you are fulfilling your promise to handle the other's confidential data. It is crucial that one person is responsible and accountable for ensuring compliance on each NDA — ideally, someone else in the organisation should be tasked with keeping track of all of them. Confirming oral disclosures requires care on both sides. If your team has disclosed information that needs confirmation, the documents must be prepared and timely delivered. If your team receives a confirmation, someone needs to check it for accuracy and provide notice of any discrepancy.

Policing limitations on use and disclosure can be awkward. Most collaborations are intended as cooperative arrangements and people will be trying to get the project done. However, these realities cannot override the need to ensure that negotiated limitations are being respected. The NDA manager should take responsibility for that task.

Action plan

Consider the following steps when factoring in trade secrets to your organisation's risk management process:.

- For IT systems, recognise that detection and response are as important as intrusion defence, and also that cyber is not the sole source of threats to information integrity. Search for weak points in management of human relationships and behaviour.
- Review your strategic plan, based on a full assessment of your information assets. Evaluate how the plan serves or fails to serve information security and exploitation, and adjust accordingly. Then take a look at whether your IP strategies are optimally balanced among the various forms of intellectual property, including secrecy.
- Review your external relationships in which confidential information is shared. Be sure that your partners have the same concerns about information security and adequate procedures to address them.
- To establish controls against the threat of infection by others' confidential information, first review your hiring practices and non-disclosure agreement management for quick fixes, then take the time to create a compliance plan that engages upper management and reinforces a culture of data security.
- Create a world-class training programme for employees that addresses their role in creating and maintaining the company's most valuable assets. Sustain it with frequency, with variation of theme and content, and with participation by management.

Ensuring post-project return or destruction of confidential records can be difficult and thankless. The clean-up work does not add to the value of the outcome and at times it can feel as though the manager is being a pest by insisting on certifications from both sides. However, leaving this unfinished is asking for trouble.

Management of intellectual property in a modern enterprise requires an appreciation of how secrecy actually works and how its risks are assessed and controlled. Although trade secrets may seem mysterious and vague relative to other forms of intellectual property, they are at the heart of how our clients create and sustain value. So understanding them fully brings us closer to the core of their business, which is its own reward. *iam*

Silicon Valley lawyer **James Pooley** is a former deputy director general of the World IP Organisation and is the author of *Secrets: Managing Information Assets in the Age of Cyberespionage* (Verus Press 2015)