IP Community Guide to Protecting Trade Secrets using Employment Law

Foreword

The Trade Secrets (Enforcement etc) Regulations 2018 brought into force EU Directive 2016/943 *on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*.

All businesses, whatever their size, hold trade secret data and this valuable data is vulnerable to online attack. In terms of the scale of this problem, research would suggest that 1-3% of GDP is lost each year to trade secret theft or misappropriation, with circa. 18% or more of that loss targeted against small and medium-sized enterprises (SMEs). Indeed a recent survey carried out by the Federation of Small Business found **5.4 million UK small businesses are collectively attacked more than 7 million times each year resulting in a staggering annual loss to the UK economy of £5.26bn**, with the Institute of Directors estimating an **average cost to SMEs of £25,000 for dealing with each cyberattack**.

When introducing this Directive the EU Commission recognised that whereas large businesses may value trade secrets as much as patents and other forms of intellectual property, SMEs value and rely on trade secrets even more. 537 firms surveyed by the EU Commission counted commercial bid documents and contracts as their most valuable trade secret data but research out of the U.S.A identifies technical information and know-how, internal business information and customer lists as the most likely trade secrets to be stolen. Furthermore, **in over 90% of trade secrets cases analysed in the U.S.A. the defendant was an employee, or former employee or otherwise a business partner**. This is why IP Wales is so indebted to Alex Christen[1] of for writing this Guide for us on protecting trade secrets using Employment Law.

Associate Professor Andrew Beale OBE
Director IP Wales

[1] Email: a.christen@capitallaw.co.uk / Tel: 02920 474 423

© Alex Christen 2018, all rights reserved.

1. Trade secrets and confidential information – the basics

Trade Secret vs mere confidential information?

Historically the definition of a trade secret was determined by case law and involved an analysis of all circumstances to see whether a piece of information could truly be classified as a trade secret. Common examples include formula, software codes and manufacturing information. Other business information was classified as 'mere confidential information', the difference between the two being the extent of the protection afforded to the business by law (see implied and express duties of confidentiality below).

The Trade Secrets Directive, which was implemented into UK law on 9 June 2018[2], introduced a new statutory definition of a trade secret as information which:

- '*is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among, or readily accessible to, persons within the circles that normally deal with the kind of information in question,*
- *has commercial value because it is a secret, and*
- *has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret[3]*'.

From an employment context, the new statutory definition makes little difference save for the third requirement for businesses to actively take steps to maintain the confidentiality of their trade secrets. Case law from the U.S. has already seen courts assessing the "reasonableness" of a companies' cybersecurity steps in terms of **identity and access management** (password protection, 'need to know' access, secure server storage); **data security measures** (USB use restrictions, distribution controls); **perimeter and network defences** (firewalls, data encryption, online use restrictions); **communication** (pop-up warnings); **monitoring** (email monitoring) (see our ***Guide to Cyber Defence***). Case law in the UK will no doubt develop but following a similar approach to that taken by companies in the US from a cybersecurity perspective can only assist.

Implied Duties of Confidentiality

During their employment, employees owe their employer an implied duty that they will conduct themselves with fidelity and good faith. The duty involves:

- acting honestly towards their employer
- disclosing to their employer all information relevant to the business
- not making secret profits from using their employer's information
- respecting confidential information belonging to their employer
- not competing with their employer's business.

[2] The Trade Secrets (Enforcement etc) Regulations 2018

[3] Regulation 2 of the Trade Secrets (Enforcement etc) Regulations 2018

© Alex Christen 2018, all rights reserved.

In practical terms, the implied duty places an obligation on employees to keep trade secrets and confidential information secret and not to use them for personal gain or in any way that would damage their employer's business. This duty is implied into all employment relationships so far as the employment relationship continues. After the employment relationship has ended, the implied duties of confidentiality will only extend to trade secrets, and not confidential information in the wider sense. For this reason, the implied duty of confidentiality only offers businesses limited protection.

Express Duties of Confidentiality

As the implied duty of confidentiality only extends to trade secrets after employment has ended (and not the wider category of confidential information), businesses should include express obligations on employees to keep business information confidential both during employment and after employment has ended (see further in section 3 below).

This is more pertinent following the introduction of the Trade Secrets Regulations as for something to be classified as a 'trade secret' (and therefore has greater prospects of being protected) the business must have taken active steps to keep the trade secret confidential.

Having an express confidentiality duty not only protects information after employment ends but it makes it far simpler to take action against an employee who breaches their express duties, which could include their summary dismissal for gross misconduct or to take action against them once their employment has ended.

Employee's skill and knowledge

Businesses can only protect information that belongs to them. Information belonging to the employee cannot be subject to restrictions. For example, the skills, experience, general knowledge and know how an employee has personally acquired throughout their career cannot belong to the business.

However in reality, the distinction between information belonging to the business and the skills or knowledge belonging to the employee is a fine one. For this reason, businesses often seek to bolster confidentiality duties by other means, for example by including an option in contracts to place employees on garden leave where their employment is ending or by using post termination restrictions (see section 3 below).

© Alex Christen 2018, all rights reserved.

2. Why employees pose a particular threat

According to a global survey undertaken by Symantec in 2012 which questioned over 3300 employees across the US, the UK, France, Brazil, China and Korea:

- 74% of employees had access to confidential information such as customer lists, employee records, financial reports and confidential business documents
- 50% of employees who changed jobs in the 12 months before the study admitted that they took confidential information with them when they left
- 40% of those employees admitted to using that confidential information to help them get a new job
- 47% of employees said their business takes action when employees take sensitive information contrary to company policy
- 56% did not believe that taking confidential information was wrong.

PwC's 2014 Global Economic Crime Survey identified the main threat to a client business as coming from an insider and the Hiscox Cyber Readiness Report 2018 confirmed that 67% of cyber insurance claims between March 2016 and September 2017 were caused by employee error.

What is clear from these studies is that employees pose a risk when it comes to protecting confidential business information and trade secrets, either by their own deliberate wrongdoing or by their accidental actions. So why is it that employees are such a risk? The following factors are relevant but by no means exhaustive:

- Changes in technology. Employees can now work from a variety of devices including mobile phones. The rise in use of social media also means that it is easier to share information with others or move information around quickly. With increased use of better technology, it is easier for information to be lost, sent to the wrong person, posted online for all to see.

- Cybercrime. Employees are considered to be a 'weak link' and easy target for cyber criminals. For example, it is quite simple for an employee who has not been trained to unwittingly click on a seemingly innocent email attachment and infect the business network with a virus. The business may then be held to ransom by the hackers who threaten to retain confidential information unless a ransom is paid.

- Flexible working options. With employees increasingly working from home or outside normal office hours, it is harder for the business to monitor its staff and fully appreciate what they are doing with business information, who they are speaking to, what security measures they have in place to keep the information secure and so on. That is not to say that employees should be prevented from working flexibly – quite the opposite. For many reasons, businesses should encourage staff to work in a way best suits them (which will in turn benefit the business). What is important however, is having appropriate measures in place to protect business information while maintaining a flexible working environment (see section 4 below).

© Alex Christen 2018, all rights reserved.

- Deliberate misuse. A current or former employee with an axe to grind, may deliberately leak confidential information or trade secrets in order to damage the business or use that information for their own personal gain.

- Employees joining competitors. Whether this would place them in breach of any contractual obligations will depend on the circumstances and the enforceability of any post termination restrictions. The employee may choose to make the move anyway and await the consequences, by which point they may already have disclosed confidential information to their new employer.

- The business' strategy on protecting confidential information and trade secrets. If a business has a strategy in place but does not enforce it, this sends a message to employees that nothing will happen if they breach their contractual obligations. Employees will be more likely to take the risk and use business information for their own gain.

The above factors are by no means exhaustive but can be mitigated against, which in turn will help a business protect its trade secrets and confidential information.

© Alex Christen 2018, all rights reserved.

3. Mitigating risk: the employment documents

Confidentiality clauses

As a bare minimum, all contracts of employment should include a confidentiality clause. For more senior positions (where the employee may be exposed to more commercially sensitive information), the confidentiality clause should be very detailed and include examples of the types of information that are important to the business. In some situations, it may be appropriate to ask employees to enter into a separate confidentiality agreement or non-disclosure as well. This might be useful if an employee is starting a new, highly confidential project or where the existing contract does not contain adequate protection.

Confidentiality clauses and agreements should not be limited to employees. Businesses should ensure there are appropriate obligations in other relationships such as for workers, consultants, contractors, interns and work placements as well as with clients and customers.

Confidentiality clauses or agreements should be carefully drafted to refer to all information that is pertinent to the business seeking to protect it. They should not be drafted too narrowly however as this may mean some information is not protected.
Wording should be clear and easy for people to understand so that there is little scope for an employee to argue they did not know what was expected of them or what the business considered to be 'confidential'.

Garden leave clauses

Another useful tool is a garden leave clause, particularly for senior employees or employees with long notice periods. They effectively give the company the option of removing the employee's access to business information for the period of their notice whilst keeping all other contractual obligations in place. A well drafted garden leave clause may also require the employee not to approach clients or customers of the business or enter company premises. The effect is that an employee can be taken out of the market and their access to new business information reduced so that by the time their employment has ended, any information they did have access to is likely to be out of date and would not harm the business if it was (accidentally or deliberately) disclosed.

Post termination restrictions

Businesses may find that it is not enough to just restrict employees' use of business information after employment has ended, particularly where it is the former employee's skill and know-how that pose a greater risk. In some circumstances it may be appropriate to include post-termination restrictions either in the employment contract or in a separate agreement.

There are several types of post termination restrictions, the details of which are beyond the scope of this note. As a rough guide a business can seek to limit employees' activities by imposing time-limited restrictions on the employee as restrictions on who they can work

© Alex Christen 2018, all rights reserved.

for, which clients or contacts they can approach or do business with and whether they can encourage colleagues to go with them when they leave.

To be enforceable, these restrictions must go no further than is necessary to protect the business and as a result, they must be carefully crafted for each business depending on a variety of factors such as the nature of the industry, the employee's role and their influence over clients and colleagues.

Policies

As well as robust contractual clauses and agreements, policies and procedures should be reviewed to ensure they contain measures designed to protect business information. For example, a confidentiality policy is a helpful way of providing a more detailed explanation of the information that the business considers confidential or a trade secret, who should have access to it, how to safeguard information and so on.

Other relevant policies include:

- An IT policy, setting out the security measures in place to protect business information.

- An email and internet use policy, explaining how the business will monitor employees' use of IT systems to ensure they are not sending confidential information elsewhere or otherwise posing a risk to the business by their unauthorised or inappropriate use.

- A data protection policy. Similar to the IT policy, this will set out the security measures in place to protect business information. It should also explain how employees should treat business information when processing it themselves.

- A social media policy making it clear that business information must not be disclosed online. The policy may also set out whether social media contacts, made during the course of employment for the benefit of the business (e.g. through LinkedIn), belong to the employee or, whether they can truly be considered as information belonging to the business. Whether in practice this distinction can be made is relevant but this should not detract a business from trying to protect such contacts.

- A disciplinary policy making it clear what will happen to employees who deliberately misuse business information.

These policies should state that they are not contractual which means they can be updated and amended by the business at any time.

© Alex Christen 2018, all rights reserved.

4. Other ways to protect business information from an employment context

In addition to reviewing contracts, agreements and policies businesses should also consider taking (and documenting to demonstrate the steps taken to protect confidential information and trade secrets) the following measures to:

- Ensure staff understand what a trade secret is and what is considered confidential information, what they can and cannot do with it and what will happen if they breach their obligations. This may be as simple as circulating a confidentiality policy and asking staff to confirm they have read and understood its contents. A better approach however would be to hold in person training sessions to ensure the message gets across.

- Provide training for staff on how they can contribute to keeping information secure e.g.:

    - Password management (i.e. using appropriate passwords to access devices, not sharing passwords with others or duplicating passwords across devices and updating passwords regularly).
    - Not using unprotected wi-fi when working remotely.
    - Guarding against leaving laptops or other devices unattended.
    - Operating a clear desk policy especially where working open plan.

- Monitor staff use of company email and internet systems. There are privacy considerations here which are beyond the scope of this note but in general, a business must make employees aware that it will be monitoring their using of company property for business reasons and explain how, why and for what purpose. Businesses should undertake a data protection impact assessment prior to undertaking monitoring and ensure they act in accordance with any email and internet use policy.

- Watch out for warning signs that staff may be leaking confidential information. For example: if staff are working long hours unexpectedly; doing unusual amounts of photocopying; spending long periods of time out of the office; or having extensive contact with customers where there doesn't appear to be the need to do so, these may be signs they are using business information for their own gain.

- Ensure appropriate action is taken in line with the business's disciplinary policy if an employee is suspected of breaching their duty of confidentiality.

- Limit access to confidential information on a need to know basis such as using encryption, password protections or require staff to log into a printer in order to access documents that may otherwise sit on the printer for anyone to find.

- Ensure anything that is confidential, or a trade secret is clearly marked as such.

© Alex Christen 2018, all rights reserved.

- Ensure staff have a basic understanding of cyber threats. They do not need to become cyber security experts but it will help if they understand the tell-tale signs of a cyber attack (such as how to identify a suspicious email or email attachment).

- Have a strategy in place on how, as a business, information will be protected and act on it. It is important to ensure that employees fully appreciate that the business will take breaches seriously and will act firmly and consistently to protect itself.

However, businesses need to undertake a balancing act to ensure that business information is protected, but not at the expense of employee relations or in a way that stifles creativity. Employees should not feel afraid to work flexibly or fear that they will be unduly punished for an accidental breach.

© Alex Christen 2018, all rights reserved.

5. Where the employment relationship ends

How the employment relationship ends will determine the best approach to take in order to protect business information. For example, if an employee resigns on good terms and the business has no reason to suspect they will use business information after they have left, it may be appropriate to simply remind them of their ongoing duties of confidentiality and any post termination restrictions at the exit interview.

If the business has dismissed the employee, as a bare minimum the dismissal letter should remind the outgoing employee of their ongoing duties of confidentiality and any post termination restrictions, give them a deadline to return all company property (including documents, laptops and phones) and require them to delete any information they may hold on a personal device and confirm to the business that they have done so.

If the employee threatens to take or takes action against the business for any claims relating to their employment or its termination, they may consider that they are no longer bound by their ongoing duties of confidentiality or any post termination restrictions. Whether this is actually the case will depend on individual circumstances as an employee will only be released from their ongoing obligations if the business has breached their contract of employment. If this happens, a business can still seek to protect its confidential information and trade secrets by entering into a new agreement with the former employee (either a settlement agreement or COT3 agreement) which will re-instate the ongoing obligations or impose new ones. Whether this is possible will depend on the situation and usually the employee will expect a sum of money or some other benefit in return.

© Alex Christen 2018, all rights reserved.

6. Summary

Actions Employers can take to protect against the 'innocent insider threat'

- Train and engage with staff on what constitutes business information and how it can be protected.
- Ensure anything that is confidential or a trade secret is clearly marked as such.
- Support employees who work flexibly to ensure they know how to and are able to protect business information outside the office.

Actions Employers can take to protect against the 'opportunistic insider threat'

- Monitor employees' use of email, phone and internet.
- Watch out for warning signs that employees may be seeking to use business information or take it elsewhere.
- Limit or restrict access to business information.

Actions Employers can take to protect against the 'malicious insider threat'

- Review disciplinary policies and procedures and ensure they specifically refer to misuse of business information as an act of misconduct and that they enable the business to take appropriate action if they suspect a breach.
- Ensure disciplinary action is taken in the event of a breach – be consistent and send a clear message that such action will not be tolerated.
- Review post termination restrictions and confidentiality clauses in contracts and take robust and consistent action for those who breach their ongoing duties.

© Alex Christen 2018, all rights reserved.

Further Reading

This Guide is intended for educational use only. For more information please refer to:

The Trade Secrets (Enforcement etc) Regulations 2018

Cyber Resilience: How to protect small firms in the digital economy (2016), Federation of Small Business

Symantec global survey 2012 – 'What's yours is mine: how employees are putting your intellectual property at risk', conducted by the Ponemon Institute in October 2012

PwC's 2014 Global Economic Crime Survey

Hiscox Cyber Readiness Report 2018, conducted by Forrester Consulting

© Alex Christen 2018, all rights reserved.