Bird & Bird

The Workforce of the Future

Business protection in a Covid-impacted world

Introduction

Employers worldwide are experiencing a period of profound change.

The Covid pandemic has significantly accelerated the advancement of digital technology and flexible working practices within organisations. The modern workplace is moving away from the traditional “nine to five” office commuter model towards hybrid systems, whether part-home, part-office, or full-time remote working.

This working revolution raises various HR, legal and compliance issues for international employers. One key challenge is how best to protect your trade secrets and confidential information in an increasingly connected and knowledge-based global economy and changing workplace environment. Where employees (intentionally or otherwise) act in breach of their duty to protect their employer’s confidential information, whether during or after their period of employment, this runs the risk of significant loss to the employer’s business including competitive disadvantage as well as financial, operational and reputational damage.

The potential economic cost and lost management time of reacting to a contentious situation after such a breach has occurred can be very high. Organisations are better placed if they take proactive steps to protect their business’ trade secrets, guard against employee breach and avoid disputes where possible. Protecting business in this way has always been high on the agenda of HR, legal and compliance teams, but is receiving renewed focus in the pandemic period. This article will look at the changing workplace environment, key areas of protection and practical steps for employers to guard their key business interests.

The changing workplace environment

We are in the early stages of a new economic and workplace environment as the effects of the pandemic period begin to take shape. The skills that businesses require from their people are continually evolving in light of digital and technological advancement. Talent needs are more complex to fulfil. Employee turnover is at record levels, referred to as the "great resignation". Reduced face-to-face engagement between companies and staff during Covid lockdowns has weakened traditional bonds of loyalty between employee and employer. There is an increasing demand for work-life balance, in particular from the upcoming generation who seek to work in a more agile and autonomous fashion. Wider job opportunities are being considered, as office workers perceive they no longer need to commute to a set location five days a week and can work flexibly from far-flung places.

This evolving business climate presents challenges for organisations when protecting their valuable assets, knowledge, and information. At the start of the pandemic, most organisations were hurriedly adapting their IT systems so that staff could work remotely and business services could still function. The emergency speed at which this happened meant that the data security implications of individuals working at home was often neglected, resulting in increased cyber attacks and breaches internationally.

For example:

- The UK Government's Department for Digital, Culture, Media & Sport reported in March 2021 that 39% of businesses had experienced cyber security breaches or attacks in the last 12 months;
- Figures from the National Cyber Security Centre showed that there were 350 reported cases of cyber attacks in Switzerland in April 2020 compared to the norm of 100 to 150; and
- Between February and May 2020 more than 500,000 people, globally, were affected by breaches where the personal data of video conferencing users was stolen by hackers and sold on the dark web.

During the Covid period, organisations across the world have been playing catch-up to provide a "cyber-safe" remote-working environment with adequate protection from cyber attacks and crime. As the "new normal" emerges, organisations must also consider security risks from their own staff and ensure that robust protection measures are in place wherever they operate. The rest of this article will focus on the key areas requiring protection and practical steps employers can take to protect themselves.

Key areas of protection

Confidential information and trade secrets

Many jurisdictions (including common law jurisdictions such as the UK and Hong Kong) have a free-standing law of confidential information and trade secrets which restricts unauthorised disclosure, whether or not there is protection in the employment contract. In the EU, the introduction of the Trade Secrets Directive (2018) has brought a degree of harmonisation to this area.

The Directive defines a trade secret as information which:

1. 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;
2. Has commercial value because it is secret; and
3. Has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

In practice, this typically covers commercially valuable information that would give a departing employee a competitive advantage, for example: customer and client information (such as identity, contact information, customer preferences and service history); employee information (including contact information, salary and bonus, job duties, training materials); processes, systems, and formulae; and operations and business plans.

The risk of misuse of such information is nothing new. For example, a notable pre-pandemic survey in the US found that:

- 50% of employees kept confidential information post-separation;
- 40% of employees plan to use confidential information in future employment;
- 60% say a co-worker has offered documents from a former employer;
- 52% of employees do not believe it is unlawful to use a competitor's confidential business information; and
- 68% of employees say their organisation does not take preventive measures to protect confidential information.

The increasingly hybrid working model is likely to exacerbate these trends. The risks of employees disclosing confidential information are increased when employees are using their own devices or are working in public places, such as cafés or co-working spaces, where third parties can eavesdrop on calls or take photographs of laptop screens, and employees may be using insecure public internet connections. Employees are taking workplace information between the office and home more regularly (whether in hard copy or electronic form), increasing the likelihood of data being lost or stolen. Remote working also provides increased opportunity for staff to leak business-sensitive information (such as client details or pricing strategy), whether deliberately or by accident.

Further, due to the loosened relationship between employee and employer and the physical distance from the workplace, employees' awareness of the confidential nature of information, or the need to protect it, can be lost; and the rise in the phenomenon known as "over-employment", where individuals perform two full-time jobs remotely at the same time, may increase the risk of employees being tempted to disclose confidential information to their 'other' employer, or inadvertently sharing copies of such information onto that other company's IT system.

Employees considering a move to a rival organisation may also take advantage of the fact that their IT activities are not monitored as closely as before and send confidential information externally or print this material at home without fear of being discovered. Employee onboarding processes for fully remote team members may be less rigorous than for "in office" employees, increasing the risks of employees bringing third party information into the organisation.

At the end of employment, the return of company property can also be slower when employees are not in the office, and remote working impacts on an employer's ability to act quickly and take immediate steps to protect its proprietary information. Employers will often only become aware of breaches after employees have gone to work for or have accepted employment with a competitor. Employers may even be inadvertently encouraging such risks by promoting a culture of constant communication and collaboration, which might encourage employees to share information using informal channels that are outside of the employer's control, such as WhatsApp and other messaging platforms.

Intellectual Property

The misuse of information by staff may also affect the intellectual property or "IP" rights of the business. These can be particularly important where the information in question is not technically confidential in the legal sense, yet still holds material value for the business. Within the EU, whilst many IP rights are harmonised, the exact scope of protection will vary between different jurisdictions and local law advice should always be taken.

Information protected by registered rights such as patents or trademarks will have been made public as part of the registration process. However, in exchange, the rights holder will have a monopoly over the product/process/mark which is the subject of the registration. Such information is very clearly protected and therefore unauthorised use of it is uncommon and can be restricted effectively.

Businesses may also be able to consider unregistered rights which are more suitable for protecting certain types of information (or parts of it):

- Copyright – Amongst other things, copyright may subsist in computer source codes, plans, diagrams, images, or databases (see below). A business will have a cause of action against any party who misuses works subject to copyright without the rights owner's permission;
- Database rights – Databases may be protected by the free-standing database right which could cover records of contacts, pricing information or other business data. Databases of contacts have traditionally been easy targets for departing employees who wish to set up in competition with their former employer; and
- Design rights – These protect against the copying of the appearance of original functional products and can be either registered or unregistered (and therefore subsist automatically). For example, a manufacturer may seek to rely on design rights to prevent another party misusing design documents or prototypes to which they have had access.

Post-termination restrictive covenants ("PTRs")

PTRs are the provisions found in employment contracts restricting the activities of a former employee once they have left the organisation by, for example, preventing them from joining a competitor and/or soliciting or dealing with former clients, customers, or colleagues for a specified period after their last day of employment. The use (and effectiveness) of PTRs differs from country to country, but in most jurisdictions, PTRs need to be reasonable in terms of their duration, their geographical scope, and must be tailored to employees' roles and activities in order to be enforceable. Fundamentally, PTRs will only be effective where there is a legitimate employer's interest to be protected.

Local law and policy changes need to be taken into account when looking at PTRs. For example:

- In some countries, compensation is required for non-compete provisions to be enforceable (i.e., clauses which prevent the ex-employee from joining a competitor for a certain period). For example, in Germany, during the period of any post-employment non-compete, employers must pay at least 50% of the remuneration that the employee received before employment ended;
- In the UK, the Government recently consulted on whether non-compete clauses should be banned or subject to compulsory compensation. This followed business concern about the UK's competitiveness in the wake of Brexit and the pandemic and a desire to drive innovation and economic recovery. To date, no changes to the law in this area have taken place;
- In Hong Kong, where courts have historically been reluctant to enforce non-compete restrictions except in a limited number of cases, the High Court recently enforced a six-month non-compete restriction, showing that the courts there are still willing to protect employers where appropriate. This acts as a deterrent for companies considering hiring new staff with such restrictions and for employees who presume that enforcement action against them will not ensue; and
- In some regions, there is specific legislation to govern the enforceability of PTRs (and other types of contractual restraint) during and after the period of employment; for example, in Australia, the Restraints of Trade Act 1976 (NSW) codifies the common law restraint of trade doctrine in the state of New South Wales.

We are currently seeing the following trends in relation to PTRs across different jurisdictions:

- As the competition for talent becomes fiercer, employers are in some cases agreeing to vary or waive proposed PTRs in the contracts for new hires (in order to incentivise them to join) and are also taking a more bullish approach to arguments against the enforceability of PTRs to which new hires are subject from their previous employer. Conversely, employers appear more willing to protect and enforce their PTRs against departing employees aggressively, leading to more disputes around PTRs;
- As companies restructure and employees take on different roles, existing PTRs may no longer be appropriate. Employers are being advised to check existing terms to consider if additional terms or new contracts are needed; and
- As global workforce mobility increases, significant numbers of employees are living and working in locations outside the countries in which they were originally hired to work. This can raise complex legal issues around whether the original geographic scope of PTRs remains appropriate, whether the PTRs are enforceable under the law of the 'new' location, and the jurisdiction in which any enforcement action should be taken.

Practical steps for employers to protect their business interests

Robust employment contracts, policies and procedures

The starting point is to check the contractual documents in place. In most countries, express wording dealing with confidential information, intellectual property and PTRs in the employment contract and relevant HR and compliance policies are the key tool available to protect the employer, in addition to relying on any implied contractual duties and protection from general law.

In certain circumstances (for example, where employees are working in particularly sensitive roles or on certain projects handling highly confidential information), in addition to the protection under their standard employment contract and relevant policies, it may also be appropriate to require them to sign separate Non-Disclosure Agreements ("NDAs") to cover the matter in question. This can serve to focus employees' minds on the importance of maintaining strict confidentiality in specific situations and act as a deterrent against potential breach.

We recommend a review of template employment contracts and relevant policies (such as Employee Handbooks, compliance manuals and IT security procedures) to ensure they are up to date and reflect the realities of the new world of remote and hybrid work, as well as any changes in the law. For example, in recent UK cases, a confidentiality clause was found to have been drafted too widely to be enforceable, and useful guidance was provided on how non-compete PTRs should be interpreted.

Suggested procedural steps include conducting an audit and risk assessment of the business' confidential information and trade secrets (including the scope of such materials, where they are held and the existing protective measures in place), keeping a record of who has control and access to such materials and making sure confidential documents are labelled as such and not for external disclosure.

Effective training, communication, and monitoring

Beyond documentation, employers should spend time educating staff about these issues through regular IT and compliance training, including on the importance of data security and the distinction between personal and corporate devices, as well as being vigilant in relation to phishing scams. As time goes on, employees may also forget what they have signed up to in their contracts, so it can be worthwhile reminding employees annually of the existence and importance of their existing contractual obligations.

More and more businesses are considering or already using technology to monitor employees' IT use. This can be effective at immediately identifying potential breaches or issues to consider; for example, irregular patterns of behaviour, including big downloads, a spike in emails to personal accounts or large volumes of printing. In most countries, monitoring systems will be subject to data protection safeguards, including whether there is a legal basis for implementing the system and any notification and consultation requirements. Organisations should also be mindful of any potential employee relations impact of introducing these tools.

Clear offboarding procedures

There are a number of measures that employers can adopt as part of the offboarding process when an employee leaves the business. These may include written reminders to employees of their contractual obligations and requiring them to confirm that they have returned all company information and property, and that they will comply with their post-termination obligations in respect of confidentiality, intellectual property and PTRs. As far as possible, devices and information should be returned by hand rather than by post, to avoid the risks of them being lost in transit or not being directed to the appropriate person or team once they are delivered.

Where permitted under the contract or local laws, putting a departing employee on "garden leave" (where they remain employed but are suspended from any active duties) can be an effective and simple mechanism for the employer to restrict the employee's activities during their notice period after they have resigned. Depending on the jurisdiction and wording of the contract, garden leave may be "off-set" against the length of any PTRs (so can act as an alternative to relying on PTRs which can be helpful if there are any concerns around enforceability). Local variations should always be taken into account. For example, in Hong Kong, employees can "buy out" their notice periods, so this should be borne in mind when considering garden leave provisions.

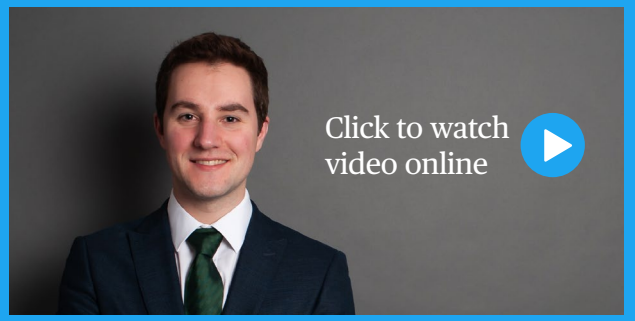
Some organisations also tie the payment of deferred compensation (such as stock options and bonuses) to employees' compliance with ongoing confidentiality duties and PTRs following the termination of their employment. Linking remuneration in this way can be a very effective deterrent and reduce the risk of breaches occurring.

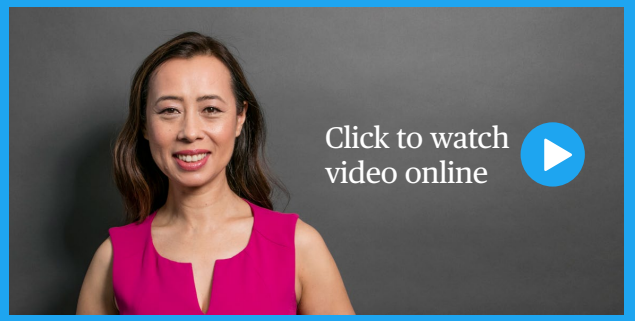
In some cases, it may be appropriate to write to the new employer to ensure that they are also aware of the individual's PTRs. In a contentious scenario, this could provide support for any subsequent claim against the new employer for inducing the former employee to breach their contract.

Conclusion

Protecting sensitive business information and trade secrets has always been a critical issue for companies, but many organisations have only re-considered their practices when reacting to a breach or damage that has already occurred. As we look to the future world of work, the challenges around business protection are becoming more complex, and organisations should make this a priority area and proactively take steps during the employment relationship and before potential difficulty arises.

Watch Rob Briggs and Diana Purdy talk about business protection in a Covid-impacted world:





Key contacts

Click for online biography

Tim Spillane

Partner, International HR Services
London

Tel: +44 20 7905 6304
tim.spillane@twobirds.com

Click for online biography

Seow Hui Goh

Partner, International HR Services
Singapore

Tel: +65 6428 9419
seowhui.goh@twobirds.com

Click for online biography

Rob Williams

Partner, Intellectual Property
London

Tel: +44 20 7415 6089
robert.williams@twobirds.com

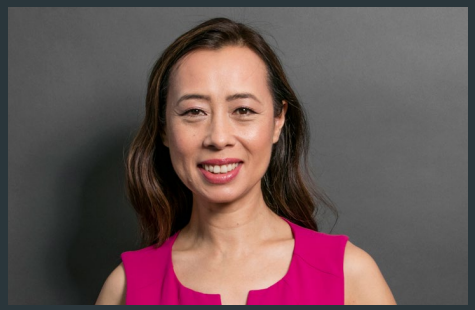
Click for online biography

Kristy Peacock-Smith

Partner, International HR Services
Sydney

Tel: +61 2 9226 9888
kristy.peacock-smith@twobirds.com

Click for online biography



Diana Purdy

Consultant, International HR Services
Hong Kong

Tel: +852 2248 6074
diana.purdy@twobirds.com

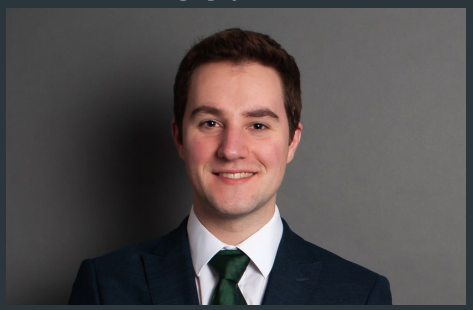
Click for online biography

Artur-Konrad Wypych

Counsel, International HR Services
Dusseldorf

Tel: + 49 211 2005 6177
artur.wypych@twobirds.com

Click for online biography



Rob Briggs

Senior Associate, International HR Services
London

Tel: +44 20 7415 6084
rob.briggs@twobirds.com

Click for online biography

Toby Bond

Senior Associate, Intellectual Property
London

Tel: +44 20 7415 6718
toby.bond@twobirds.com

twobirds.com