Alan Adcock
Partner and Deputy Director, Intellectual Property
alan.a@tilleke.com

The Risk of Trade Secret Misappropriation during Work-from-Home Arrangements

While we've all seen how quickly life has changed during the pandemic, from a business and HR angle the possibility of intellectual property misappropriation and theft occasioned by work-from-home policies may not yet be clear to many. With many employees working outside their company's normal IT security fence, their increased use of their own computers and devices, instead of those in their offices with standard or enhanced security mechanisms, has made it more challenging for employers to control access to key business information.

In the rush to set up a fully or partially remote workforce, most companies had little time to establish work-from-home guidelines on protection of their valuable intangible assets like trade secrets and confidential business information. Most employers would likely have sufficient internal guidelines on copying files to USB drives, emailing files to personal accounts, and uploading to cloud storages like Dropbox, Google Drive, or OneDrive, but who could have imagined the need for rules precluding sharing proprietary information over Zoom, Skype, Webex, House Party, Ring Central, or Microsoft Teams?

In addition to misappropriation by employees, many organizations have also seen hackers exploit vulnerable IT protocols and bait people with emails related to the current health crisis. Phishing and ransomware emails have been used to lure people working from home in attempts to access protected systems. Hacking of smart home devices has resulted in recordings of confidential conversations being transmitted to not only Amazon, Google, and other providers but to hackers and thieves as well.

Given this background, there are a couple of important steps that employers should take to start protecting themselves from theft (either intentional or not) or to enhance existing protocols.

HR Tasks

First, each employer should speak to the company's HR team to make sure they understand the existing workplace rules regarding the handling and maintenance of confidential business information. Now is the time for HR to revisit existing rules and update them for the new normal. This should include a refresher in employment agreements or individual confidentiality agreements (particularly important for key personnel) to accommodate work-from-home realities. In order to successfully prove a case against a trade secret infringer, the owner must show demonstrable evidence that all reasonable care was taken to maintain the confidential information. This would include regular reminders to employees about what is meant by "confidential information" or "trade secrets" and their duty to maintain that confidentiality if they are allowed access.

Employee sharing of business information has accelerated with the increased adoption of some of the platforms mentioned above. While many employees would already be familiar with a company's rules on disclosing to third parties, such as doing so only under a written non-disclosure agreement, this is complicated with the new ways in which we are all now communicating outside our companies. Document sharing can be controlled by secure transfer tools like password-protected FTP programs, time-limited document viewers, and limitation of the number of downloads.

For businesses in the unfortunate circumstance of having to lay off or furlough employees because of the pandemic, work-from-home realities make the exit interview even more important. In addition to existing requirements such as return of all company property (including loaner devices used from home), HR will want to secure additional undertakings, such as assurances that no unauthorized copying or downloading occurred on any device, no company information is retained in any form, and no confidential information was shared with third parties without proven authorization. Also, if the departing employee was a member of any R&D, design, or engineering team, an enhanced exit interview is an ideal time to effect IP assignments or other declarations necessary to vest all employee-created IP or improvements in the employer (preferably before termination). Even if the research project is incomplete, this might be a good time also to consider filing provisional patent applications with the employee's written further assurance that subsequent follow-on applications will not be jeopardized.

IT Tasks

Employers should also talk to the company's IT team about existing security measures and any necessary enhancements. The IT team will be well placed to complement the HR efforts described above by updating existing security measures, implementing new ones, and explaining any changes to employees. This might include a new personal device use policy (or "bring your own device" policy) with an explanation of the employer's right to track and monitor its own devices as well as those of the employee who uses them for their work—all legal in Thailand, as it is in most jurisdictions around the world so long as employees are made aware. IT would likely also find this an ideal time to install new or updated antivirus, spyware, and malware protections. Personal devices will be much more at risk of hacking than fenced-in company IT architecture, so the IT team should install necessary security on personal devices as well if these are to be used for company work outside the workplace. If employees are allowed VPNs or other remote access platforms as a backup to the business network, employers should decide whether to place any restrictions on downloading, copying, or transferring files.

While no business can completely insulate itself from leakage of its proprietary information, most can take steps to significantly reduce the risk, mitigate damage, and prove that reasonable care was taken to protect their property. In these unique times, the best internal teams employers can turn to for assistance in establishing the necessary safeguards are HR and IT.