THAILAND

The risk of trade secret misappropriation while working from home continues

Tilleke & Gibbins
Bangkok

Alan Adcock

With many employees in Thailand 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 have had little time to establish work-from-home guidelines on protection of their valuable intangible assets like trade secrets and confidential business information. The need for sufficient internal guidelines on copying files to USB drives, emailing files to personal accounts, and uploading to cloud storage is already widely recognised, but who could have imagined the need for rules precluding sharing proprietary information over Zoom, Skype, Webex, and such programs?

In addition to misappropriation by employees, many organisations 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.

HR tasks

A top concern for companies in Thailand should be revisiting rules for handling and maintaining confidential business information. This should include a refresher in employment agreements or individual confidentiality agreements (particularly for key personnel) to accommodate work-from-home realities. To prove a case against a trade secret infringer, the owner must show that care was taken to maintain the confidential information. This would include regular reminders to employees defining "confidential information," "trade secrets," and their duty to maintain confidentiality. Many will already be familiar with a company's rules on information disclosure, but this is complicated by new patterns of external communication, often involving online collaboration and meeting tools. For document sharing, companies might employ secure transfer solutions like password-protected FTP programs, time-limited document viewers, and limitation of the number of downloads.

For businesses forced to lay off or furlough employees, work-from-home realities make the exit interview even more important. Along with existing requirements such as return of company property, companies should secure additional undertakings, such as assurances that no unauthorised copying or downloading occurred, no company information is retained, and no confidential information was shared without authorisation. If the departing employee was on an research and development, design, or engineering team, an enhanced exit interview is an ideal time to effect IP assignments or other necessary declarations. Even if the research project is incomplete, companies might consider filing provisional patent applications with the employee's written assurance that follow-on applications will not be jeopardised.

IT tasks

The IT team can complement these HR efforts by updating existing security measures, implementing new ones, and explaining changes to employees. This might include a new personal device use 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 so long as employees are made aware. Personal devices will be at greater risk of hacking than fenced-in company IT architecture, so the IT team should also install necessary security on personal devices used for company work. If employees are allowed virtual private networks (VPNs) or other remote access, employers should decide about potential restrictions on downloading, copying, or transferring files.

While no business in Thailand can completely insulate itself from leakage of proprietary information, most can take steps to significantly reduce the risk, mitigate damages, and prove that reasonable care was taken to protect their property.