Bangkok Post The world's window on Thailand

CORPORATE COUNSELLOR

IT law update (PART 1): The Cybersecurity Bill

Published: 23/01/2015 at 06:00 AM
Newspaper section: Business

Earlier this month, the cabinet approved a series of bills related to information technology, personal data, cybersecurity and telecommunications. One such bill would recast the Information and Communication Technology Ministry as the Digital Economy and Information Technology Ministry to reflect the importance of IT in Thailand's economy — the same rationale behind the entire set of bills. This article focuses on one of these bills, the cybersecurity bill. Next week in a follow-up article, we will discuss another one of these bills, the bill to amend the Computer Crimes Act.

Given recent events, governments around the world are focusing on threats occurring over the internet as well as attacks using computing equipment and networks and how to counteract these threats to improve overall security. Thailand is no different. The cybersecurity bill, as approved by the cabinet, would establish a National Cybersecurity Committee and a new state agency, the Office of the National Cybersecurity Committee, to focus on these issues.

The committee would have the responsibility to determine how to respond to serious cyberthreats, effectively to serve as the centre of operations in the event of an IT calamity (save for matters of military security) and cooperate with other state bodies and private entities for this purpose, among related responsibilities. The Office of the National Cybersecurity Committee would be responsible for implementing the committee's policies as well as related responsibilities specified in law.

The bill also features a reporting mechanism for state agencies and/or designated persons in each agency to provide information to the secretary of the committee so it could determine what further actions to take in response to particular cyberthreats. Further, where maintaining cybersecurity is necessary — for example, in a case where there may be an effect on financial and commercial stability or national security — the committee may even order a state agency to take particular actions and report as the committee may instruct.

It is envisaged that the minister overseeing the committee would appoint officials to perform certain roles. These officials in turn may be authorised by the secretary of the office to request a state agency or any person to give testimony, submit a written explanation or submit materials for inspection or information — all within the scope of the Act — or request state agencies or private entities to facilitate the committee's performance of its duties.

The bill also would empower officials to access communications information, be it in the form of posts, telegrams, telephones, faxes, computers or any mechanism or device for electronic communication or telecommunications, for the purpose of cybersecurity. However, it also contemplates that the cabinet would specify rules for officials to follow in accessing such information, presumably for the purpose of addressing privacy concerns.

The law also contains provisions to protect such information and to prevent its disclosure except in cases of prosecution under the Act, abuse of power or as otherwise authorised by a court.

The most controversial provision of the bill relates to accessing personal communications content. Indeed, commentators around the world have expressed concerns about access to personal communications by state agencies of various countries. These concerns are understandable and legitimate. Nevertheless, current public discourse seems to reflect that policymakers' concerns about terrorism and national security are outweighing traditional concerns about personal privacy.

In Thailand, the practical reality is state agencies already have access to communications content under a variety of other laws. Hence, the provisions in the cybersecurity bill do not substantially expand the state's ability to access such information. Rather, in the larger picture the bill would seem to envisage the establishment of a framework for such access.

All countries need to focus on cybersecurity, and the cybersecurity bill lays out a framework for this in Thailand. The reality is that it is impossible to predict all possible cyberthreats that may arise, which is why the bill gives effect to plans and policies to be adopted by the National Cybersecurity Committee. In that regard, the success of the bill will ultimately depend on those plans and policies, which would be expected to undergo continual adjustment and updates to meet current threats.

In next Friday's article, we will discuss the proposed changes to the Computer Crimes Act — changes that may be a cause for concern for some.

This article was prepared by David Duncan, consultant, and Jeffrey Blatt, counsellor, in Tilleke & Gibbins' corporate and commercial department. Please send comments to Andrew Stoutley at andrew.s@tilleke.com