

Complying with the Computer Crime Act

The Computer Crime Act applies to all businesses in Thailand.

Bangkok Post, Database, p. D6, April 2, 2008.

TIMOTHY BASS



Thailand's Computer Crime Act (CCA) was a major milestone towards lowering operational risks related to computer crime. After some initial comments by industry, the government provided clarification and guidance, stating that the intent of the CCA is to cover all businesses in Thailand that provide Internet access, not just Internet Service Providers (ISPs). So, in a nutshell, if an organisation has a website or provides access to the Internet for their employees or customers, it has specific responsibilities under the CCA.

Specifically, businesses must be in a position to provide Internet-related records to authorised officials as they investigate cybercrime in the Kingdom. Therefore, one of the main requirements of the CCA is that companies must keep records of Internet access and traffic for a minimum of 90 days, and for up to one year if requested.

If you think about it, this makes perfect sense. For example, if an employee is using the office email system to send out threatening emails to someone, the company must be ready, willing and able to provide records of such emails to the authorities. Likewise, if an employee breaks into their company's customer database and steals private data, the company must be able to provide computer system access records to authorities.

This means that just about every business with Internet access has a very important legal responsibility to the community under the CCA. If something happens, and the authorities come knocking on the door for computer records, and a company cannot provide these records, it could be subject to a fine up to 500,000 baht. In addition, if the authorities find that a company has intentionally supported a cybercrime, as defined by the CCA, then that company can receive the same criminal penalty as the person or persons who committed the crime. This could result in imprisonment of up to twenty years, if the crime resulted in the death of someone.

Companies are beginning to understand the importance of the CCA and are investigating how they can comply. Naturally, small businesses that do not use the Internet, or provide Internet access, have little or no responsibility under the CCA. On the other hand, companies that are ISPs, which includes Internet cafés, have specific responsibilities under the CCA.

Hotels, apartment complexes and condos that provide Internet access to their employees also have the responsibility to ensure that proper records are kept, if their Internet service provider has not already done so. It might be good for these organizations to check to see if their ISP is in compliance.

For large companies with many employees, it is imperative that they review their policies, procedures, processes and technologies to ensure that they keep proper records of both computer access and actions by their employees. The more computer systems and Internet access points a business has, the more responsibilities it has under the CCA.

For example, the Bank of Thailand (BOT) provided the excellent Guideline for Security of Electronic Services (BOT Notification No. 2848-2546, November 19, 2003). This means that commercial banks, finance and securities companies in Thailand should already have in place most of the safeguards and controls that lead to compliance with the CCA. It would be a good idea for these businesses to review the CCA to learn how policies, processes and technologies are affected and what changes, if any, needs to be made.

Businesses are working hard to comply with the CCA, and are interested in how the CCA impacts their existing risk management responsibilities. Organisations often go a step further and like to assess and improve their IT security to international security standards such as ISO 27000.

Although these standards can seem overwhelming for many busy IT security departments, it is helpful to know that there are similarities and overlaps between the ISO security standards, the BOT Notifications, and the CCA. These standards provide an excellent baseline for teams to assess how prepared they are for that dreaded "knock on the door" when an official wants to see a company's internal access control records, as well as the logfiles of computer and Internet access for the last three months.

If you, a member of your family, or your business were ever to be a victim of a cybercrime, you would expect nothing less than full compliance with the CCA when authorities are searching for records and evidence related to the crime. The CCA is for everyone's benefit, and that includes you.

Contact Us

David Old
Partner
david@kpmg.co.th

Siraporn, Chulasatpakdy
Partner
schulasatpakdy@kpmg.co.th

Pavit Mekmok
Executive Director
pavit@kpmg.co.th

Timothy Bass, CISSP
Executive Director
tbass@kpmg.co.th