Bangkok Global Law
540, Unit 1705, 17th Floor, Mercury Tower,Ploenchit Road,
Lumpini, Pathumwan, Bangkok 10330 Thailand
Tel: +(66) 2 2525895-6 Fax: +(66) 2 2525897
Website: www.bgloballaw.com
E-mail: info@bgloballaw.com

Thailand's Cybersecurity Bill Pushes Duties Beyond CII Operators

Thailand is considering significant draft amendments to the Cybersecurity Act B.E. 2562 (A.D.2019) that could broaden cybersecurity obligations beyond organisations formally designated as Critical Information Infrastructure (CII). The National Cyber Security Committee (NCSC) has released the draft amendments for public consultation, after which they are expected to proceed to the Cabinet and the Parliament for consideration. Among the proposed changes are a clearer distinction between a "cyber threat" and a "cyber threat incident", expanded incident-reporting obligations for certain private-sector organisations, greater oversight of external service providers to CII organisations, and the addition of the industrial sector as a new CII category. The proposals remain draft legislation and are not yet in force.

One of the most consequential changes is the potential expansion of cyber incident reporting beyond the existing CII framework. Private-sector organisations to be identified under future subordinate regulations could be required to report incidents that affect or may affect cybersecurity, including matters connected with national or military security, economic security, international relations or public order. Failure to make a required report without reasonable grounds could attract criminal penalties. The practical scope of this obligation will therefore depend heavily on the organisations and incidents ultimately prescribed by implementing regulations.

The draft would also extend the reach of cybersecurity regulation indirectly to vendors serving CII organisations. CII operators would be required to oversee and monitor external providers for compliance with prescribed cybersecurity standards and the Cybersecurity Act. If a provider fails to remedy non-compliance within 60 days, the NCSC could require the CII organisation to consider discontinuing the relevant service. The NCSC would also notify government agencies, relevant regulators and CII organisations of non-compliant providers, effectively establishing a regulatory blacklist. Notably, the proposal as described does not provide the service provider an opportunity to respond before being placed on that list.

These measures reflect the increasing dependence of critical operations on third-party technology and outsourced infrastructure. Cybersecurity risk no longer sits solely within the systems directly operated by a regulated organisation; vulnerabilities may arise through cloud services, enterprise software, AI solutions, maintenance providers and other external technology relationships. By placing responsibility on CII organisations to supervise their vendors, the draft would use procurement and contractual relationships as an additional regulatory channel. The proposed inclusion of the industrial sector as a CII category would further broaden the range of businesses potentially brought within Thailand's heightened cybersecurity framework.

From a legal and business perspective, the amendment could significantly reshape cybersecurity compliance for technology vendors as well as regulated operators. Cloud providers, software companies, AI service providers and outsourcing businesses supplying CII customers may find cybersecurity standards incorporated into service agreements, tenders, terms of reference and purchase orders even where those vendors are not directly designated as CII organisations. Businesses should therefore monitor the legislative process, future subordinate regulations and the eventual scope of the blacklist mechanism, while reviewing incident-response procedures and vendor-management arrangements. Until the amendment is enacted, however, these requirements should be treated as proposed reforms rather than existing legal obligations.

Should you have any question, please do not hesitate to contact us via info@bgloballaw.com