Amendment to Cybersecurity Law in Singapore (Cybersecurity (Amendment) Bill No. 15/2024)

Cybersecurity and data protection have become an essential part of any business. Earlier this month, a bill passed by the Singaporean parliament aimed to strengthen the country's cybersecurity measures in response to evolving threats. Under amendments to the Cybersecurity Act, owners of critical information infrastructure (CII) are now required to report a wider range of cybersecurity incidents, including those within their supply chains.

Adapting to Emerging Threats

The new law allows for the regulation of Systems of Temporary Cybersecurity Concern (STCC) and Entities of Special Cybersecurity Interest (ESCIs), which are deemed critical to Singapore's national interests. Notably, The definition of “computers” will include virtual systems and cloud infrastructure that are increasing in usage.

Addressing Modern Challenges

The amendments aim to address operational challenges faced by regulatory authorities in light of technological advancements and evolving cyber threats. As Singapore continues to navigate the evolving cybersecurity landscape, the updated laws seek to ensure the country remains resilient against cyber threats while fostering a secure digital environment for its citizens and businesses.

Bearing the above in mind, we see three (3) key takeaways.

Amendment to Cybersecurity Law in Singapore (Cybersecurity (Amendment) Bill No. 15/2024)

Expanded Reporting Requirements: Service providers and businesses need to be aware of the expanded reporting requirements outlined in the new legislation. Owners of critical information infrastructure (CII) are now mandated to report a wider range of cybersecurity incidents, including those within their supply chains. This reporting obligation extends to other computers that are under the owner's control, as well as computers under the control of a supplier that are interconnected with the CII.This means that businesses need to ensure they have robust mechanisms in place to detect, investigate and report cybersecurity incidents promptly and accurately.

Regulatory Changes Affecting Operations: The regulatory changes introduced in the Cybersecurity (Amendment) Bill will have significant implications for the operations of service providers and businesses. These changes include the introduction of new regulatory frameworks for Systems of Temporary Cybersecurity Concern (STCC) and Entities of Special Cybersecurity Interest (ESCIs), as well as updates to CII-related provisions. Service providers and businesses must familiarize themselves with these changes to ensure compliance and adapt their operations accordingly, in particular, (a) the Responsibility for Virtualized CII, and (b) Third-Party Vendor Requirements.

Emphasis on Cybersecurity Preparedness: The Bill underscores the importance of cybersecurity preparedness in the face of evolving threats and technological advancements. Businesses need to recognize the critical role they play in safeguarding Singapore's national interests and take proactive measures to enhance their cybersecurity posture. This may involve investing in advanced cybersecurity solutions, strengthening internal protocols and procedures, and staying updated on emerging cybersecurity trends and best practices.

Contact us to learn more.

+65 8617 7787

tradekins.com

connect@tradekins.com