Cybersecurity & Firewalls

Overview

While most are familiar with the “Great Firewall of China,” the Chinese government’sInternet censorship against foreign websites and unfavorable speech, people are lessfamiliar with what part this firewall plays in the intricacies of China’s cybersecurityregime. President Xi Jinping While most are familiar with the “Great Firewall ofChina,” the Chinese government’s Internet censorship against foreign websites andunfavorable speech, people are less familiar with what part this firewall plays in theintricacies of China’s cybersecurity regime. President Xi Jinping emphasized on multiple occasions that the Internet poses new challenges for China’s interests andthat the government is rightly empowered to dictate the measures securing thoseinterests. On November 7, 2016, the government promulgated a new set ofcybersecurity measures against the protest of numerous foreign businesses. Thesemeasures are aimed primarily at network providers who provide services thegovernment determines crucial to the operation of services on the Internet, alsoknown as “critical information infrastructure.” The law will require the providers tosubmit to an invasive security review and store any data collected from the users inChina within the geo-graphic boundaries of China. This policy enables China’sregulatory agencies to exercise wide discretion in determining which providers fall into what category, and what precise measures need to be taken to satisfy thelegislation. While China is not alone in creating such a state-controlled cyber-securityregime, the broad authority it gives to itself is notable, leaving little for non-government entities to do but obey. multiple occasions that the Internet poses newchallenges for China’s interests and that the government is rightly empowered todictate the measuring those interests. On November 7, 2016, the governmentpromulgated a new set of cybersecurity measures against the protest of numerousforeign businesses. These measures are aimed primarily at network providers whoprovide services the government determines crucial to the operation of services onthe Internet, also known as “critical information infrastructure.” The law will requirethe providers to submit to an invasive security review and store any data collectedfrom the users in China within the geo-graphic boundaries of China. This policyenables China’s regulatory agencies to exercise wide discretion in determining whichproviders fall into what category, and what precise measures need to be taken to satisfy the legislation. While China is not alone in creating such a state-controlled cyber-security regime, the broad authority it gives to itself is notable, leaving little for non-government entities to do but obey.

Technical Details

The Framework’s most interesting feature is its use as a common language for entities involved in cyber infrastructure to evaluate their current posture, determine a targeted state, and assess their progress towards that targeted state. It operates through a process that utilizes three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profile. The Framework Core provides asset of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. It is a non-exhaustive list of industry-specific best practices for managing cyber risk and uses a com-mon terminology that allows for organizations to communicate more effectively. These practices are sorted into Informative References, which are placed at the bottom of a sorting hierarchy, from Function, to Categories, to Subcategories, and finally to the Informative References.