China Cyber Security Law update

China's goal to control cross-border data flows is now impacting multinational companies' operations

New data flow enforcement impacting MNC's China operations

Regulators are moving to impose tighter control over internet services that companies may use to connect to outside of China, including VPNs and webservers. The operational impact of this development could impact:

- Access to local email via web pages
- Remote access to files and folders hosted on servers in China
- Connections between China offices and offices/data centres outside of China

While enforcement of licensing requirements by telecoms companies is notable in of itself and the expected blocking of site-to-site VPNs is a long-dreaded further tightening of China's internet controls, this development is consistent with China's goals in controlling both information flow and the technologies that deliver it.

Unlicensed services are being blocked

During the fourth quarter of 2017, in three eastern Chinese cities, two different national telecoms companies delivered letters to their Chinese and MNC customers explaining that without a proper licence, all data traffic to specific ports[1] will be blocked.

In some cases telecoms providers did not give any advance warning. Control Risks spoke with some organisations regarding the sudden disruption of their on-premises web operations. The application of the regulations (and blocking of data traffic) was only discovered when IT support teams contacted the telecoms provider as part of the troubleshooting process.

In late 2017, Control Risks spoke to multiple members of the MNC business community about recent problems with certain types of VPNs. They reported the blocking of their cross-border IPSec VPN services[2] (a common corporate VPN) between their China locations and offices/data centres abroad. This was initially expected to be short term disruption, timed to coincide with the 19th Party congress. However, the problems have persisted and align with the

1 These "ports", part of the addressing system for internet traffic, are those used by webservers to provide unencrypted (HTTP, port 80) and encrypted (HTTPS, port 443) access to a web site. Port 8080, often used by IT teams to support a secondary web service on a server, is also specifically mentioned in the letters.

2 IPSec (Internet Protocol Security – a collection of open source protocols) is a common technology to create and maintain a secure, encrypted connection between two locations such as a remote office and a data center. It uses UDP ports 500 and 4500 as channels over a network.

planned closing of certain ports. Control Risks expects that IPSec site-to-site VPNs with connections outside of China will be blocked in the near future.

What does this mean for our clients in China?

Clients operating any kind of on-premises service accessible from the internet (e.g. websites, VPNs) should ensure that the service is properly licensed.

- All on-premises web servers require an internet content provider (ICP) bei'an (ICP备案) licence.[3] This licence is issued by the Ministry of Information and Information Technology and local Public Security Bureau, and must be registered by a Chinese national. A similar licence is required for e-commerce websites (ICP Zheng, ICP经营许可证).
- Established IPSec VPNs or software-defined wide area networking (SD-WAN)[4] should be considered "at-risk". They are likely to be blocked in the near future and may not be reliable for critical business functions.
- Clients should consider alternative connectivity solutions such as leased lines and MPLS. These will be provided directly or indirectly[5] by a local telecoms provider and should be appropriately licensed through the contracting process with the provider.
- While VPN connectivity over the internet in China is restricted, companies who wish to ensure the security of their wide area connections may wish to operate a VPN within the leased line/MPLS with an appropriate security architecture at both ends of the connection.

How can Control Risks help?

Control Risks is a specialist global risk consultancy that helps organisations succeed in an age of ever-changing risk and connectivity. Through insight, intelligence and technology, we help you seize opportunities while remaining secure, compliant and resilient. When crises and complex issues arise, we help you recover.

Control Risks provides risk advisory services on policy, regulation, cyber security and compliance relating to China's cyber security law. We help MNCs understand where enforcement is headed and develop cyber security, crisis management, and operational strategies to respond to this evolving and complex regulatory landscape.

We would be happy to further this explain this development and potential responses. Please feel free to contact our team should you have questions:

Control Risks CSL team

Carly Ramsey in Shanghai	carly.ramsey@controlrisks.com
Ben Wootliff in Hong Kong	ben.wootliff@controlrisks.com
Jim Fitzsimmons in Singapore	jim.fitzsimmons@controlrisks.com

[3] While this has been required for some years and is necessary for external hosting of a website, it is now definitively required for local hosting of web servers.

[4] SD-WAN solutions mimic the stability and functionality of conventional dedicated line wide area networks, but operate over local internet connections. While they are an effective and increasingly popular solution for companies, they still run over a network and whatever port they may use to establish and/or maintain a connection can be blocked.

[5] Irrespective of the contracting entity, all wide area networking solutions (leased lines, MPLS, etc.) are delivered physically and operated by a local Chinese telecoms company.