Why HR Should Care about VPN Use in China

By **Alexander Chipman Koty**, **China Briefing**, **Dezan Shira & Associates**

Word Count: 1338

The "**Great Firewall**", the popular term for China's Internet restrictions, blocks access to a large swathe of the internet, including Google, Facebook, YouTube, Twitter, and many other overseas news outlets and social media platforms. Internet users in mainland China can bypass the Great Firewall by using VPNs, which reroute internet activity through servers based in another location.

For many companies and individuals in China, VPNs are necessary to perform a number of basic tasks, from sending emails via a Gmail account to sharing resources through **cloud platforms** like Dropbox and even GitHub. For some companies, the ability to use a VPN enables them to carry out their core functions, such as desktop research and digital marketing.

Despite the inconveniences, most businesses in China are accustomed to navigating the Great Firewall as a necessity of doing business. However, recent legal and regulatory developments – namely the sweeping new **Cybersecurity Law** and a campaign to "clean up" the Internet – have called into question the status quo of VPN usage in China.

Regulation of VPN use

Operating and using VPNs has long been a legal grey area in China. In the past, Chinese authorities have periodically cracked down on unlicensed VPN operators based in China, while deploying various methods to limit access to overseas VPNs and curtail their effectiveness.

This orthodoxy surrounding China's cyberspace has been challenged by the introduction of the Cybersecurity Law, which came into effect on June 1, 2017. The far-reaching law includes strict **data localization** and network security requirements, and vastly increases the government's overall regulation of cyberspace.

Furthermore, in early 2017, China's Ministry of Industry and Information Technology (MIIT) announced a "clean-up" of China's internet, which included references to VPNs. Since then, popular China-based VPNs, such as GreenVPN and Haibei VPN have been shut down or have suspended their operations, and app stores, including the Apple Store, have removed VPNs from their mainland China platforms.

Additionally, unlicensed VPN sellers have received tougher penalties than ever before. In one particularly harsh case, a man from Guangxi was sentenced to jail for five and a half years and fined RMB 500,000 (US$76,923) for operating and selling VPNs without a license.

For the most part, it is operators and sellers of VPNs that are punished, rather than individuals and companies that use VPNs. However, the possibility of punishment for VPN use exists.

For example, in early 2017, the Chongqing government warned that individuals could be fined up to RMB 15,000 (US$2,308) for using “illegal channels” to bypass the Great Firewall. Despite this announcement, Chongqing officials later stepped back and said it was a restatement of regulations dating back to 1996. It does not appear as though this warning has been enforced.

Corporate VPN use in China

Contrary to popular belief, it is legal to both operate and use VPNs in China under certain conditions. For example, it is possible to apply to the government to offer VPNs for commercial purposes, which are accessed via state-owned telecommunications companies, such as China Telecom and China Unicom.

Companies in China can use these VPNs for internal business purposes but, officially, must maintain a VPN usage record. Using a government approved VPN administered by a state-owned enterprise is, however, not attractive to most companies due to security and privacy concerns.

More commonly, international companies establish their own corporate VPNs for internal use, which connect a company’s China operations with other overseas locations. Companies worldwide frequently use such systems to communicate and share files securely, even if they do not need to bypass internet restrictions.

Companies that operate internal VPNs for business purposes have not been the targets of VPN crackdowns to date. However, cyberspace authorities may still interfere with the effectiveness of such VPNs incidentally as they routinely detect and suppress VPN connections in general.

Smaller companies that do not have the infrastructure to set up internal VPNs often purchase corporate VPN subscriptions from overseas providers. Connections from these providers can be interfered with when accessed from within mainland China, but these providers cannot be entirely shut down since they are based outside the country.

HR implications

As VPNs – and internet usage, more broadly – have come under the microscope of government authorities in recent years, HR practitioners face a greater need to establish internal controls to deal with a tighter – and fluid – regulatory environment.

When establishing HR processes for VPN use, HR should liaise closely with IT to gain a deeper understanding of how VPNs work and how IT can configure systems in accordance with HR protocols. That being said, HR management of VPNs in China begins with internal company rules for internet use and acceptable workplace behavior.

In China, employees may be tempted to use a corporate VPN for personal use in the workplace, as many people either lack access to a VPN at home or do not want to spend money on paying for a service. Employees might use their employers’ VPNs not only for accessing blocked websites like YouTube or

Bloomberg, but could also engage in activities that are illegal, such as pirating movies, which could pose a risk to the business in the form of legal action.

To ensure that VPNs are only used for business purposes and not for personal use, VPNs should only be installed on company-owned devices. Furthermore, each employee should be given unique login credentials to access the VPN, and be made aware that their internet use will be logged and could potentially be monitored. Internal policies relating to employee internet use can be included in the **company handbook** and presented to employees by HR practitioners during onboarding.

Businesses should also take into account the productivity considerations of reliance on VPNs. Due to government interference, VPNs may at times be rendered ineffective, thereby preventing employees from carrying out key tasks. Inability to use a VPN may not only disrupt work, such as research and digital marketing, but also communication with other offices and clients.

VPNs are known to come under more pressure at politically sensitive moments, such as during important political meetings or when a scandal is being reported in the news. For practical purposes, however, it is impossible to predict when a VPN will stop working effectively.

If VPNs are necessary for core business functions, businesses should establish contingency plans for the event that their internal VPN stops functioning. This might be a “backup” subscription to a third-party VPN provider for key personnel, or a deeper infrastructural IT fix, depending on the nature and needs of the company.

Companies that are expanding into China for the first time should conduct an internal review to identify how they may be affected by the Great Firewall. While it is well known that many major news and social media websites cannot be accessed in China, new entrants may be surprised by the breadth of other software and applications that can be affected, particularly for cloud-based services.

Monitor regulatory developments

To date, the Chinese government’s “clean-up” of VPN usage has primarily consisted of shutting down unauthorized operators and sellers within mainland China and making it harder for individual users to access VPNs for personal use. Meanwhile, the Cybersecurity Law increases the government’s remit to regulate cyberspace and gives it the authority to investigate companies’ network usage and IT infrastructure.

However, these developments have not fundamentally altered the unspoken understanding that companies can use VPNs for internal business purposes. Yet they do raise the possibility that VPN use in the future will be increasingly channeled through official mechanisms, i.e. state-owned telecom providers, and that companies’ digital behavior may be monitored more closely.

Cyberspace and VPN use are sensitive areas in China. Corporate VPN use continues to exist in a legal grey area where it is neither explicitly forbidden nor permitted. Companies should therefore monitor government announcements and media reports to detect any shift in policy and enforcement to prevent disruption of normal business operations and potential legal issues.

This article was originally published in the April 2018 edition of the **Hong Kong Institute of Human Resource Management***'s Human Resources Magazine.*

This article was first published on China Briefing.

Since its establishment in 1992, Dezan Shira & Associates *has been guiding foreign clients through Asia's complex regulatory environment and assisting them with all aspects of legal, accounting, tax, internal control, HR, payroll, and audit matters. As a full-service consultancy with operational offices across China, Hong Kong, India, and ASEAN, we are your reliable partner for business expansion in this region and beyond.*

For inquiries, please email us at china@dezshira.com*. Further information about our firm can be found at: www.dezshira.com.*