China Briefing
From Dezan Shira & Associates

Securing Your China Remote Work Strategy Against Internet Vulnerabilities

Written by Alexander Chipman Koty, **China Briefing**, **Dezan Shira & Associates**

The COVID-19 coronavirus outbreak has launched an unprecedented level of remote work arrangements and the digitalization of business operations in China and worldwide.

Due to lockdown measures to combat the spread of the virus, hundreds of millions of people across the world are suddenly working from home. Even as life in China gradually returns to normal, many China-based employees are now finding themselves communicating with clients and coworkers overseas who are now working remotely.

The proliferation of remote work arrangements raises a number of logistical and security concerns for businesses in China. Unreliable international internet connections have become an even more visible issue than normal, while maintaining network security – especially for remote workers – is now a pressing issue. Further, the sudden adoption of new video conferencing technology as part of the transition to remote work arrangements has introduced new security and productivity concerns for employers.

Here, we identify and offer solutions for three common IT challenges that businesses are facing in China amid the COVID-19 pandemic.

Improving internet performance in China

The COVID-19 outbreak has accelerated the digitalization of day-to-day business functions for firms that had not done so already. One consequence of digitalization,

however, is that firms may find their networks overloaded and, in particular, face inconsistent speeds when communicating with international servers.

Because of China's Great Firewall, international internet traffic is essentially funneled through just three submarine optic fiber entry/exit points, located in Qingdao, Shanghai, and Shantou. As a result, international internet speeds in China tend to be highly inconsistent.

International internet access is particularly slow during high-usage hours of the day, as traffic gets clogged while waiting to be filtered. This applies not only to websites and services blocked by the Great Firewall, but anything hosted on a foreign server.

Slow and inconsistent internet is a common frustration that can lead to dropped calls with employees and clients, among many other situations. On a macro-level, it can be a significant strain on a firm's productivity when employees are hampered by an uncooperative internet connection.

To solve these common issues, businesses in China can enlist an internet service provider that offers specialized packages in handling international traffic. Companies such as CDS can set up systems to optimize connections with international servers – ensuring higher levels of speed and reliability than normal providers – all without significant changes to network infrastructure.

Improving company network security

Since the COVID-19 outbreak is necessitating remote work arrangements at an unprecedented scale worldwide, there has been an uptick in phishing attacks and security breaches. At the end of March, for example, the US cybersecurity software company MonsterCloud reported an 800 percent increase in calls for assistance.

With hundreds of millions of people working remotely worldwide, hackers and cyber criminals are trying to take advantage of employees working on personal unprotected networks and devices lacking adequate security. Moreover, hackers can potentially gain more valuable data than usual, as many workers communicate online sensitive information that they would normally only discuss in person.

In addition to standard phishing emails that impersonate clients and coworkers, among others, during the coronavirus pandemic hackers have impersonated government bodies and even the World Health Organization, purporting to be conveying emergency health information.

Accordingly, businesses are recommended to conduct a network security audit to determine the effectiveness of their current security practices and identify areas of vulnerability. By analyzing, studying, and gathering network data, a network security audit can assess levels of vulnerability and offer fixes for lapses that might emerge.

In addition to analyzing the technical aspects of network security, a security audit can also asses a firm's IT policies surrounding employee behavior and best practices. Network security breaches often occur not due to inadequate technology, but because employees are not trained in proper security protocols or because the firm lacks standard policies to guide employee behavior online.

Video conferencing vulnerabilities

With employees being forced to work from home to comply with lockdown measures, businesses are turning to video conferencing programs like Zoom to conduct meetings that would normally be held in person. Some of these programs, however, come with various privacy and security concerns.

Users have cited a number of issues with Zoom, for example. Zoom reportedly shares users' data with Facebook and does not provide the end-to-end encryption it advertises, while Mac users are reportedly vulnerable to webcam and microphone hijackers. Another security concern is the practice of so-called "Zoombombing", where uninvited users join a meeting.

In addition to these issues, some of Zoom's built-in features have raised concerns. For example, Zoom allows meeting hosts the ability to track attendees' internet usage, which raises privacy concerns with employees.

Moreover, the international version of Zoom is blocked in China by the Great Firewall. There is a local Chinese version, which is run in partnership with the Chinese telecom

company Huawan Telecom. Despite this, the connection can be unstable when communicating with international users.

In light of these concerns, businesses may instead opt to use a program such as Microsoft Teams, which has a more proven record of security and privacy. Many businesses already use the Microsoft 365 suite for other functions, such as Microsoft Outlook, which makes the integration of Teams seamless.

In addition to offering video conferencing, Teams also provides other productivity tools designed for remote collaboration, such as scheduling and file sharing tools. Further, Microsoft software carries a strong reputation of working well in China, even when communicating with international users.

For more information on conducting a network security audit, solving IT challenges, and securing a smooth remote work transition in China, please contact our IT specialists at Dezan Shira & Associates.

This article was first published by China Briefing, which is produced by Dezan Shira & Associates. The firm assists foreign investors throughout Asia from offices across the world, including in China, Hong Kong, Vietnam, Singapore, India, and Russia. Readers may write to info@dezshira.com for more supp