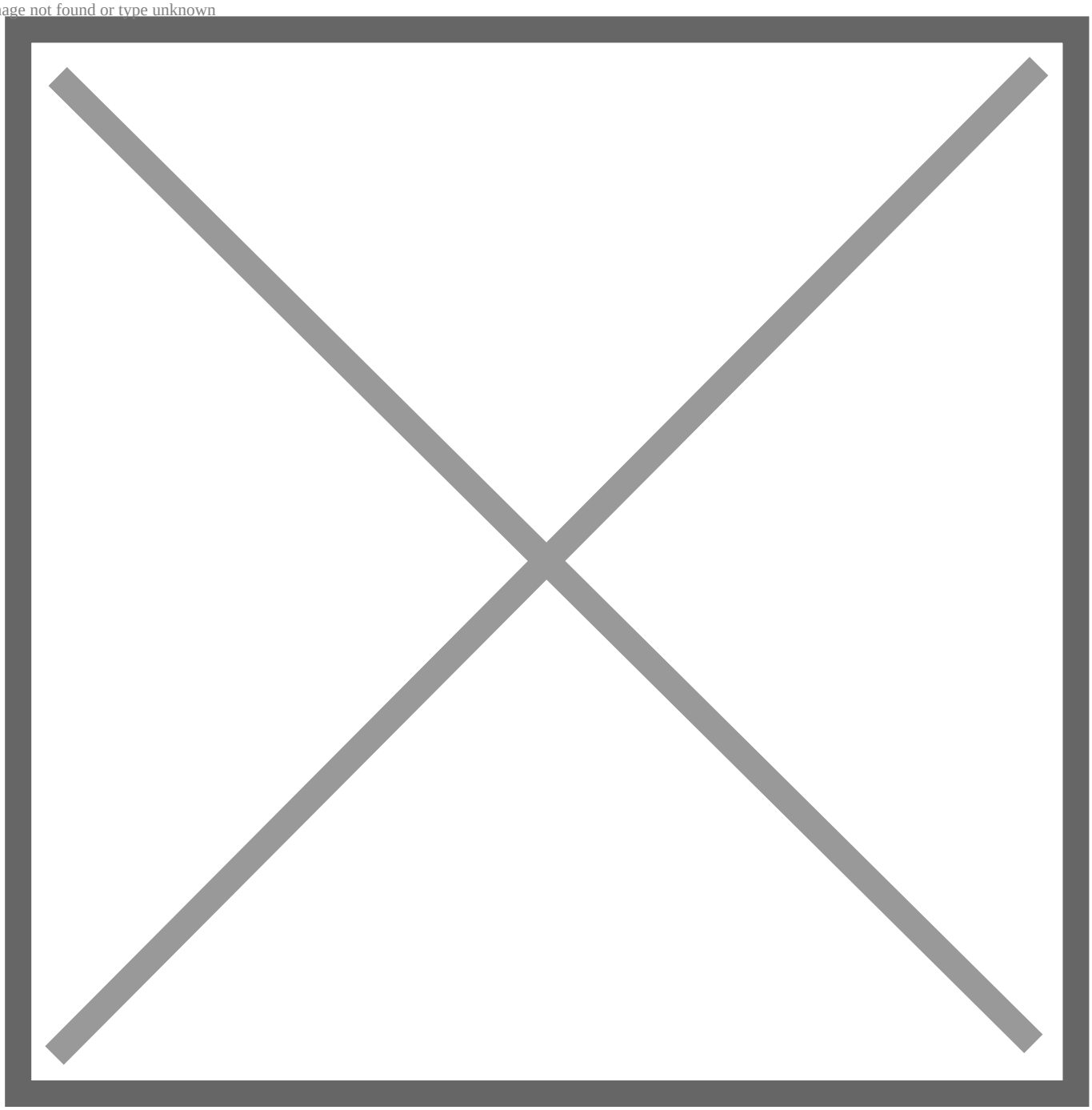
Cybersecurity in China: What You Need to Know

TAGS | Information and Communication Technology (ICT) | Cybersecurity

ARTICLES | 4 March 2015

Image not found or type unknown



China has the largest online population with about 642 million online users. More remarkable though is the fact that some other half a billion people in China are not yet connected and still can join the club of connected netizens. China's online population has great potential to thrive in the

digital era.

Through the rise of low-cost smartphones and expanded internet connectivity in particular, more and more Chinese are expected to come online.

It is estimated that 60% of the Chinese netizens have already been browsing the web with their smartphones. They use the online world for activities such as shopping (e-commerce), communicating (social media), or entertainment (online gaming).

As a result, tech companies are benefiting greatly from this trend, such as the smartphone producer Xiaomi, one of the world's most valuable start-ups.

Yet the stakes are high.

In 2013, cybercrime caused damage worth $37 billion in China. As more Chinese netizens use mobile payment systems, cyber criminals will seek golden opportunities to hack into these financial systems and its devices.

It seems that without profound IT knowledge, individuals, SMEs, big enterprises, and governments, are likely to become easy victims of expanding cybercrimes.

What does that mean for SMEs? Two questions are especially important to understand.

1. How can SMEs in China defend themselves against cybercrime?

Though media coverage on cyber incidents such as hacking, IP theft, and espionage is mushrooming and despite the fact that governments are increasing their focus on "cyber" issues, SMEs are still not investing enough in cybersecurity.

A study by the Ponemon Institute in 2013 has found out that only 58% consider cybersecurity relevant for their businesses and that 42% do not invest enough in their IT security.

A reason might be that in cyberspace it is much easier to attack than to defend. And not everyone is tech-savvy enough to understand the complex technical processes.

Other than just investing in IT security software, there are some basic tips that can help SMEs prevent major cyber incidents from happening. For instance, it is essential to train your staff in cybersecurity: Most cyber intrusions can be prevented if your staff is well trained and aware of the various cyber risks. This is especially important to SMEs that tolerate BYOD practices (bring your own device).

2. What efforts are currently undertaken by the Chinese government?

The Chinese government wants a "healthy development" of its internet. It wants its cyberspace to be clean of "spiritual pollution" (online rumors or pornography). As a result, strong internet regulation policies are being enforced in order to gain sovereignty over cyberspace. To the disadvantage of foreign SMEs in China, access to foreign websites and their digital services are blocked or being restricted (Facebook, YouTube, Google, Microsoft Windows).

This leads to the effect that local firms will shape the digital landscape in China. Most of them will offer similar services that mainly target the Chinese audience, and some will eventually offer innovative services. Overall, the Chinese government believes that advanced digital technologies will lead to more innovations that aid economic growth.

As the decline of Western digital services in China continues, SMEs in China should strengthen their efforts to better understand the Chinese digital market with its blooming service providers, but also beware of the inherent risks.

On the one hand, SMEs can look out for great business opportunities by using and trying out new IT services. On the other hand, local Chinese IT newcomers still need to prove that they can offer quality services, great customer support, and security; the risks are that the chosen company might become a failed investment and might even negatively disrupt business operations.

(This article is provided by Karsten Luc, Director of Operations, Think Asia Group)