What To Know About China's New Cybersecurity Inspections

By **Jordan Kelly** (May 31, 2019)

Jordan Kelly

In November 2018, China introduced new provisions — "Regulations on Internet Security Supervision and Inspection by Public Security Organs" — to a previously enacted cybersecurity law from 2017. These provisions allow, among other things, Chinese state agencies to perform remote penetration tests on any organization operating in China that conducts internet-related business and uses more than five internet-connected computers. The Chinese Ministry of Public Security is responsible for conducting the remote penetration tests.

The MPS also now has the authority to conduct in-person network security inspections, search for content that is prohibited in China and prosecute unlawful content possession, copy user information that is discovered during an inspection, share data with other state agencies, record how organizations implement response plans during in-person inspections, and have the People's Armed Police present to enforce the investigation.

What Does This Mean?

The nature of this law means applicable organizations are susceptible to inspection. Unplanned external network access can damage networks and machines, interrupting business continuity, or worse, cause irreversible effects. An e-commerce business would lose revenue every second that their website is offline, and a company that relies on their databases for everyday tasks would see operations screech to a halt if they're unable to access them.

Even if the remote access does not disrupt systems or networks, it can expose valuable intellectual property or reveal proprietary practices of interest to competitors. This is information that businesses rely on being kept secret, otherwise their competitive advantage dissolves, and unplanned penetration tests have the potential to put this important information at risk. Gaining access to a network also creates an opportunity for undesired surveillance.

Similarly, client data also faces exposure via remote inspection. Through the new cybersecurity provisions, the Chinese government maintains the right to copy client information without providing clear details on what they can do with it. The language included in the new law does not specify exactly whose data can be copied — whether it is any data that is discovered during an inspection, or just data controlled by Chinese citizens. If copied customer data is stored in another location outside of the primary business, this is a potential new entry point for hackers to steal this valuable information.

Regardless of the main function of a business's operations, an unplanned network penetration test puts their business continuity and critical assets at increased risk, creates additional opportunities for third-party data breaches, and leaves them potentially unaware that an intrusion occurred and that anything was affected as a result.

How to Mitigate Risk

It is essential to first consider your business's relationship with China and think about the

potential impact that exists. Do you have critical assets stored on networks operating in China? Do you qualify to be subject to an inspection? Do your products or services involve hosting content prohibited in China? If so, you should determine what steps can be taken to prepare for a potential investigation.

This may include segmenting your operations so that networks, databases and systems functioning in China are not connected to those functioning elsewhere in the world. This will help ensure that inspections are conducted only where this authority exists. A security architecture assessment can help determine the layout of your digital ecosystem and what may need to be changed to avoid unnecessary inspection.

It's possible that the MPS will take a similar approach to conducting their investigations as to what is commonly seen in data breaches — the path of least resistance. Malicious actors often scan for known vulnerabilities and utilize them as easy points of entry. Instead of trying to "break in," the MPS will first check if the front door is unlocked. Vigilant patch management — which should already be included in any organization's security plan — will prevent easy access via known vulnerabilities.

Additionally, it is necessary for businesses operating in China to understand the local laws they are subject to follow. Depending on what kind of data your organization handles, it's possible that you must meet additional requirements to ensure compliance. In the event that an inspection does take place, you don't want to face potential compliance failure or associated steep penalties. Addressing regulatory requirements is a necessary aspect of any risk strategy, but its importance is further brought to light when faced with the potential of an unplanned inspection.

Lastly, you must develop a plan proactively so that your organization and its employees are not caught off guard with the introduction of an inspection. Instead of trying to react in real time, build out processes that define your response team (i.e., who interacts with the MPS inspection team), the role of each employee during the inspection, who you need to contact (i.e., outside counsel), and what your communications strategy involves (i.e., interacting with customers and dealing with media inquiries). This will reduce business interruption and maintain customer confidence.

A Growing Trend

Similar to the California Consumer Privacy Act, the provisions to China's Cybersecurity Law are part of a larger trend of regionally based regulations and laws that have recently been implemented. Increased attention to topics such as data privacy concerns and consumer protections has helped jump-start this trend. Companies that operate globally need to be cognizant of laws and compliance requirements that pertain to specific regions in the world.

Neglecting these new laws can have serious consequences. In January 2019, the French Data Protection Authority issued a fine of €50 million against Google Inc. for violating the EU General Data Protection Regulation. Although the decision is currently being appealed by Google, it's evidence that international companies will be held responsible for maintaining compliance.

China's new provisions may not carry the same potential for a hefty fine, but for businesses operating there, the additions to the law create another area of cybersecurity that requires attention. This type of due diligence should already be included as part of your overall security process regardless of where your business operates.

Assess, Defend, Identify, Respond, Recover

State-backed agencies have the resources and the means to gain access to almost any network or database they please, and the reality of China's provisions to their Cybersecurity Law is that they now have the legal right to do so to businesses operating in their country. The key to risk reduction relies on implementing a set of core fundamentals — cyber hygiene — combined with staying current with cybersecurity trends.

The cyberthreat landscape evolves rapidly, and your policies need to keep pace with emerging risks. Through building a robust security posture, which includes assessing your relationship with global governments, organizations can take steps to reduce the reach of the new provisions and prepare for potential unplanned inspections.

Jordan Rae Kelly is senior managing director in the cybersecurity practice at FTI Consulting Inc. Previously, she served as the director for cyber incident response on the National Security Council at the White House.