COVINGTON

Cyber Crime in Brazil: Preparing for the Rio Olympics

July 11, 2016

Data Privacy and Cybersecurity

The Brazilian financial industry has long been a target of cyber criminals, and with the continued growth of sophisticated online banking services in Brazil, such systems are a prime target for organized crime. In addition, among the emerging BRICS countries (Brazil, Russia, India, China, and South Africa), Brazil is on par with China and Russia in terms of internet usage by the population; of particular note is the widespread use of social media and mobile devices. Given this ubiquitous connectedness, users and companies are regularly targeted by online attackers, primarily for financial gain, but also increasingly to commit cyber espionage and hacktivist disruptions.

Given the historic levels of cybercrime in Brazil, the heavy economic reliance on the financial and telecommunications industries, and the widespread use of the Internet, the Federal police and other government agencies also have fairly sophisticated cyber capabilities. In more recent years, the government increasingly has focused its efforts on cyber warfare and anti-terrorism, particularly as it relates to detecting and preventing attacks on critical infrastructure and Brazilian-hosted worldwide events, such as the Olympics and World Cup.

In short, Brazil is a high-risk destination with respect to cybercrime, particularly online banking, and the risk will only be heightened by the influx of travelers and businesses into the country for the Olympics. Consequently, to reduce the threat of being victimized, companies conducting business with or within Brazil, and personnel traveling to Brazil, must be vigilant and take precautions when transporting data and other assets to Brazil, and engaging in online business while in Brazil. It is incumbent upon such companies to adequately train their employees and provide the tools necessary for them to protect valuable assets/data and themselves.

Accordingly, we provide the following best practices as guidance:

- When possible, leave your devices at home; instead, bring a laptop loaner or swap out your hard drive. Similarly, use a disposable phone and create a temporary email account with a unique password.
- Back up all critical data before you leave.
- Make sure your antivirus protection is up-to-date, and software is fully patched with the most recent security patches/updates.
- Disable all computer functions that you don’t need, including, for example, Bluetooth, thumb drive access, and cameras.
- Minimize the use of credit cards, social security numbers, and the sharing of other sensitive data, including passwords, over the Internet while in country.

- Encrypt all data in storage (encrypt your device with whole disk encryption) and encrypt data/communications in transit.
- Use secure corporate VPNs whenever possible, and otherwise use HTTPS connections and sites.
- Keep your computers and devices with you at all times. Physical crime is also rampant in Brazil.
- Assume that all connections may be monitored, including your hotel room phone, and avoid sensitive data transfers and communications.
- Hotel networks and computers are particularly vulnerable, and should be avoided when possible. Also avoid using other publicly available computers (those found in libraries, internet cafes, etc.).
- Be aware of shoulder-surfing (i.e., reading data on screens over your shoulder or when you are away from your computer), including at ATMs.
- Change your passwords both before and after your trip; reinstall the OS and/or otherwise dispose of the device.
- Notify your banks and credit card companies regarding your travel; report any lost/stolen credit cards or devices as soon as possible.

Also, be aware that export control laws, or local foreign laws, may prohibit the transport of particular software or technology, including encryption technologies, or prohibit the use of certain tools in country. In addition, although Brazil generally recognizes a right to privacy online, both foreign *and U.S. border control agents* may require you to present your devices for inspection, including directing you to decrypt data stored on those devices.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our firm:

Jenny Martin +1 212 841 1018 jrmartin@cov.com