


# GLIMPSE INTO: INTERNATIONAL CYBERSECURITY

Here is a glimpse into the International Cybersecurity map we created. For a more detailed version including key concerns, laws, and initiatives in even more countries, please contact us. We are happy to send along the poster sized version.

Crimes in cyberspace will cost the global economy **\$445 billion in 2016** according to an estimate from the World Economic Forum's 2016 Global Risks Report. Threats will increasingly come from China and Russia, however, US companies have more than just cyber threats to be concerned with when it comes to international business. US companies also need to be mindful of foreign regulations and guidelines dictating privacy and data protection, which in places like Europe, are more stringent than in the US. Here are the top data protection and cyber security items to keep in mind in each region.



## EUROPE - Privacy Shield

- Privacy Shield is a proposed framework for transatlantic exchanges of personal data for commercial purposes between the European Union and the United States.
- US companies that receive personal information of EU member states must take steps to insure they are in compliance with the new directive.
- US companies also must have processes in place to address privacy complaints in a timely and effective manner.

## LATIN AMERICA - Lack of Cybersecurity Plan

- 80% of countries in Latin America lack a cybersecurity strategy or plan to protect critical infrastructure (*The 2016 Cybersecurity Report by Inter-American Development Bank*).
- A large majority of prosecutors in Latin American countries lack the capacity to punish cybercrime.
- American companies with offices and business in Latin America must rely on their own set of standards and security measures to limit incidents.

## **RUSSIA** - Hackers

- It is not just the Democratic National Committee that has to worry about threats from Russia. Russians have proven even more adept than the Chinese in some instances of hacking US systems, including the electrical grid.
- Russian and Ukrainian hackers were responsible for one of the largest hacks in the history of the United States. It cost companies over \$300 million in bank-card fraud from 2010 to 2013.

## **CHINA** - Private Corporate Data

- In January of 2016, a new Chinese law went into effect that requires any Internet or telecomm company in China to provide law enforcement with technical assistance, including decrypting sensitive user data to investigate terrorism.
- More than 40 global firms with business in China are actively fighting another new law. The law creates government security reviews that could threaten the protection of intellectual property. The law also introduces strict requirements to keep data in China that will make it hard for international businesses to conduct standard operations.

## **JAPAN** - Act on the Protection of Personal Information

- Japan has recently updated regulations with the Act on the Protection of Personal Information (APPI). The APPI protects things like biometric codes and codes for goods and services.
- An entity can transfer data outside of Japan only if the country has similar legal requirements to Japan or the company demonstrates that it has met specific privacy requirements.