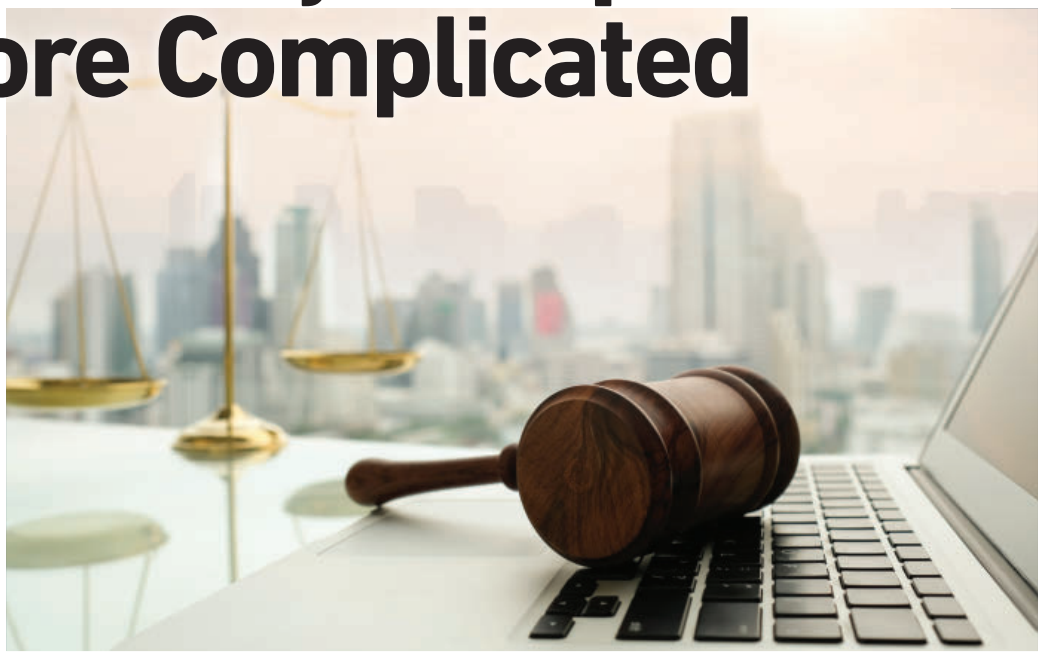
# Cyber Security Compliance Gets More Complicated

China's new data protection regulation, in addition to laws enacted by the U.S. and EU, has huge implications for any business with international exposure.

**By Alex Wright**



***Myriad state and national data protection regulations*** complicate cyber compliance for all companies.

***U.S. companies that do business abroad*** or handle overseas data will now have to comply with a host of new cyber security rules after China became the latest country to impose regulations on firms operating there.

This follows hot on the heels of the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which came into force in the U.S. in March, and the European Union's (EU) General Data Protection Regulation (GDPR), introduced two months later.

The implementation of these new protocols is driven by the recent surge in cyber attacks and, in the case of China, greater protectionism, exacerbated by the U.S. trade war, as the world becomes more divided than ever before.

Now, even if you are U.S.-based, you could be affected by a law in a country thousands of miles away. To date, 117 countries now have cyber security laws in place, not to mention each U.S. state having its own rules.

That has only led to greater ambiguity and conflict between the different regulations, increasing the burden and cost of compliance for organizations.

For many companies, these greater regulatory requirements have forced them to scale back their activity in certain countries, and in some cases, they have pulled out altogether.

"There's a big call to action by governments to be seen to be doing something to protect their citizens, but it's not being done in a way that's consistent," said Shannon Groeber, JLT Specialty's cyber and E&O practice leader. "It's a real challenge for companies operating on a global scale to make sure that they understand all of these new regulations and how they differ from country to country, or even state by state.

"Added to that, for many companies it seems that as soon as they have got up to speed with a new regulation, another one is introduced that they have to comply with," she said.

## THE SECOND GREAT WALL OF CHINA

China's new cyber security law, enacted in June, requires organizations operating in critical sectors such as finance, telecommunications and transport to store personal information and business data in the country, provide unspecified "technical support" to security agencies and pass national security reviews. It also stipulates that data must not be transferred overseas without government approval.

> ***"There's a big call to action by governments to be seen to be doing something to protect their citizens, but it's not being done in a way that's consistent"***
>
> ***— Shannon Groeber,*** *cyber and E&O practice leader, JLT Specialty*

Penalties for violations range from a company's business activities being suspended and its website shut down to its forced closure or loss of license. The maximum fine for an offense is RMB 1 million ($150,000).

Carrie Yang, assistant vice president and team leader of Aon's Cyber Solutions Group, said the new law significantly increases the cost of compliance for companies. It also exposes them to far greater regulatory action, she said.

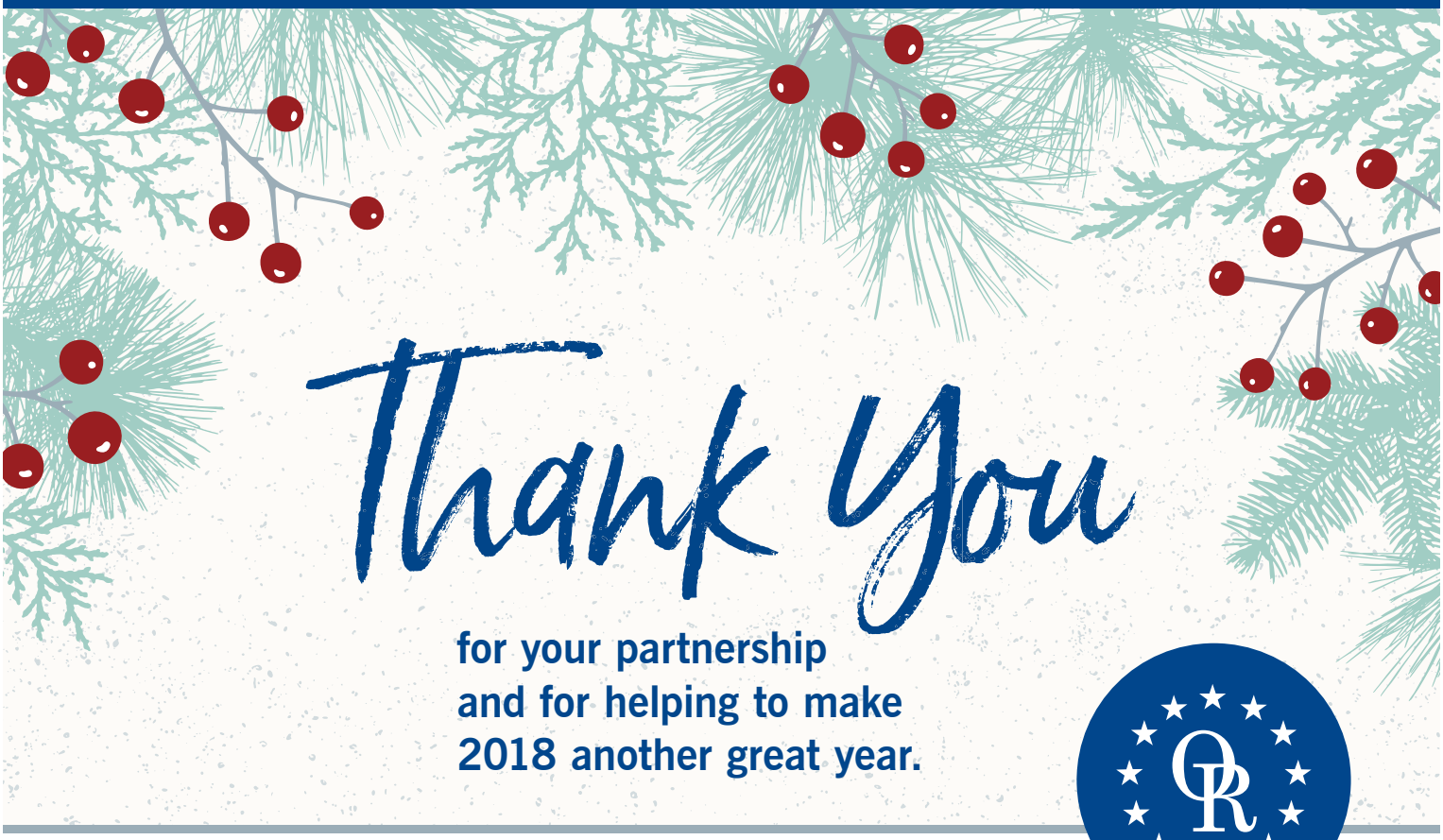
"Companies will now have to adhere to much stricter rules requiring them to conduct local cyber security assessments, obtain local certification and have in place a local cyber security and compliance team," she said. "We are also hearing anecdotal evidence that organizations have already been subject to informal regulatory inquiries under the new cyber security law."

As recently as last month (November), Yang said that China introduced a new regulation on the Internet Security Supervision and Inspection, which gives the country's police sweeping powers to inspect company networks onsite and remotely. It also requires firms to carry out

## SUMMARY

- ***China*** is the latest country to enact cyber security regulations.
- ***Greater regulatory requirements*** forced some companies to scale back activity in certain countries.
- ***Noncompliance can result*** in criminal investigations and massive fines.

# OLD REPUBLIC INSURANCE GROUP




## Old Republic General Insurance Group

BITCO Insurance Companies[1]
Great West Casualty Company
Old Republic Aerospace[2]
Old Republic Contractors Insurance Group[3]
Old Republic General Insurance Corporation
Old Republic Home Protection Company
Old Republic Insurance Company
Old Republic Insured Automotive Services[2]
Old Republic Professional Liability[2]
Old Republic Residual Market Services
Old Republic Risk Management[2]
Old Republic Specialty Insurance Underwriters[4]
Old Republic Surety Company
PMA Companies[4]

*We wish you a healthy, happy, and prosperous new year.*

Insurance contracts are underwritten and issued by: 1. BITCO General Insurance Corporation and BITCO National Insurance Company; 2. Old Republic Insurance Company; 3. Old Republic General Insurance Corporation; 4. Pennsylvania Manufacturers' Association Insurance Company, Manufacturers Alliance Insurance Company, Pennsylvania Manufacturers Indemnity Company.

**orgig.com**

security breach assessments, she said.

"It has huge implications for companies doing business in China, as well as increasing their exposure to third party liability," she said. "The biggest challenge, however, will be how to protect their intellectual property and confidential information."

Roy Hadley, cybersecurity attorney for Adams and Reese, said this increased scrutiny exposes companies to a greater risk of their information being misappropriated, shared with competitors or used by the Chinese government. In response, many have announced plans to separate their Chinese operations from the rest of their business by transferring data to government sponsored data centers, he said.

"The bottom line is that many global companies doing business in China are worried that under the broad wording of the new law and their compliance obligations, their trade secrets, proprietary information and data are now subject increasingly to oversight by the Chinese authorities, including possible misappropriation," he said.

"Any international company needs to be very careful about operating in China and about how to protect this crucial information while simultaneously complying with the law."

Kevin Richards, Marsh Risk Consulting's global cyber risk consulting leader, said in the event of a criminal investigation, firms need to work with Chinese law enforcement and provide full access to data and unspecified "technical support" upon request. They must also store data gathered or developed in China on local servers and it must not be transferred abroad without government permission.

"Data sovereignty is a big topic for a number of countries — so that part isn't new — but it does limit the types of service providers or cloud services firms that are available for use," he said. "Minimally, companies will need to review their external vendor contracts to assure that they can achieve this 'data sovereignty' requirement."

## GDPR AND THE CLOUD ACT

GDPR is the biggest overhaul of the EU's data privacy policies in more than 20 years, standardizing data protection across all 28 member states and governing the control and processing of personal information. It applies to any company that accesses data from EU-based users, even if they don't physically operate in any of the member states.

The maximum penalty for a violation is a fine of up to €20m or four percent of a company's global annual turnover, whichever is higher.

Karen Schuler, BDO USA's data and information governance leader, said GDPR served as a wake-up call to organizations to get their privacy policies in line with global standards. To comply, she said, some even went as far as to set up data centers in the EU.

"In certain cases, companies have decided it may be easier to comply with GDPR by opening up data centers in the EU," she said.

***"Companies will now have to adhere to much stricter rules requiring them to conduct local cyber security assessments, obtain local certification and have in place a local cyber security and compliance team."***

**— *Carrie Yang,*** *AVP and team leader, Cyber Solutions Group, Aon*

"Regardless, now when boards consider how their organizations can keep pace with mounting data-related challenges, their priority should be building a culture of privacy, with cyber security and regulatory compliance as critical components."

The CLOUD Act requires U.S.-based technology companies to provide data stored on servers in any jurisdiction if requested by Federal law enforcement. Last year New York also brought in tough new cyber security rules for banks, insurers and other financial institutions.

But Annie O'Leary, assistant vice president of Aon's Cyber Solutions Group, believes that the California Consumer Privacy Act, slated for 2020, will have a much bigger impact on companies.

The new law will put much greater restriction on the collection and use of personal information by companies, she said.

"Essentially it provides a number that a third-party individual can file if there's damage due to loss of their information or any breach," she said. "For any company operating in the state that handles citizens' data, that's a huge concern."

## GLOBAL COMPLIANCE

In order to comply with these new laws, companies need to ensure their cyber security policies and IT systems are up to speed, including carrying out risk assessments. They must also have the appropriate incident response and business continuity plans, as well as insurance coverage, in place.

Richards added companies need to have an ongoing and robust cyber regulatory readiness program in place that helps them understand the different jurisdictional requirements.

They must also maintain regular dialogue with their internal information security leadership and corporate counsel to keep up to date and review their cyber security policies, he said.

"A good starting point to maximize the utility of corporate cyber security policies is to map existing policies to one of the current internationally recognized security frameworks," he said.

"The main two are the International Organization for Standardization ISO 27,000 series and the U.S. National Institute of Standards and Technology Cyber Security Framework." **&**

## California Consumer Privacy Act

The California Consumer Privacy Act of 2018 was signed into law by Governor Jerry Brown in June. California is the first state to pass its own data privacy law.

Likened to the European Union's GDPR, the law, which comes into effect in 2020, will give consumers greater control over their personal data.

It will enable them to see what technology companies like Facebook and Google are collecting, why they are collecting it, who they are sharing it with and request for it to be deleted.

They will also be able to discover whether organizations are selling their information to third parties, such as advertisers, and to request them to stop doing so.

Consumers will be able to bar companies from selling their data, and children under 16 must opt in to allow the collection of their information.

Organizations found mishandling data could be fined up to $7,500 for each violation.

**ALEX WRIGHT** is a UK-based business journalist and former deputy business editor of The Royal Gazette in Bermuda. He can be reached at riskletters@lrp.com