

View this article on our website:

[http://www.agendaweek.com/articles/20100517/  
boards\\_balance\\_opportunities\\_china\\_with\\_increasing\\_risks](http://www.agendaweek.com/articles/20100517/boards_balance_opportunities_china_with_increasing_risks)

Here's the article:

---

---

## **Boards Balance Opportunities in China With Increasing Risks**

Article published on May 17, 2010

By Tony Chapelle

Multinational corporations that do business with China are increasingly getting caught up in counter-surveillance to protect their trade secrets.

Directors need to be briefed on the implications for their companies and make sure their managers take steps to protect technology and other intellectual property.

In January, Britain's spy chairman reportedly warned that telecommunications giant BT could be shut down by China and that Britain's power, water and food supplies could be cut off. Alex Allan sent out a confidential document, according to London's The Timesnewspaper, that accused Chinese telecom maker Huawei Technologies of having supplied BT's new communications network with components that could bring down the system.

"Mitigating measures are not effective against deliberate attack by China," Allan stated in the report.

Last December, Google was hit by a two-day cyber attack from inside China that opened a directory of information about the work tasks of Google employees. The breach also may have given the government

access to the Gmail accounts of human rights activists inside the country.

“Companies doing business in China need to be especially concerned about surveillance by the government,” says Donna Boehme. Formerly the chief compliance officer at BP, she now operates a compliance consulting firm called Compliance Strategists.

The stakes have become serious. Last month, the National People’s Congress made changes to the 21-year-old law governing state secrets.

The new law, which will take effect on October 1, could be troubling. It requires companies to pass on information, or spy, on persons, companies and even customers and employees that divulge state secrets. There is no specific definition for such secrets, Boehme says, although the term could include maps and economic statistics.


Some reports claim that the law could boost China’s high-tech companies against foreign competition.

One governance observer claims that IP theft is rampant by many countries beyond China. Government agencies often actively assist domestic commercial businesses in stealing foreign corporate secrets, writes Nir Kossovsky in an e-mail. Kossovsky is executive secretary of the Intangible Asset Finance Society. He wrote the book, *Mission Intangible: Managing Risk and Reputation to Create Enterprise Value*.

In fairness, Kossovsky adds, the U.S. steel and textile industries were built on the back of British trade secrets. “Historically, less developed nations lift IP from more developed nations until they, in turn, become generators of original IP. Then these new innovator nations move to strengthen IP laws and security.”

For U.S. corporations, the primary governor on IP theft is that the U.S. is a major market for most goods that might contain American-produced

intellectual property. The law here allows customs agents to confiscate products that infringe upon patents and copyrights at the border.

 Kossovsky says that this governor becomes moot when it comes to trade secrets, however. U.S. laws set penalties only for American citizens who steal IP, and only within the U.S.

The tightening of the Chinese secrets law comes on the heels of China's convictions of four executives of the British-Australian mining company Rio Tinto. In March, the four were found guilty of stealing corporate secrets and accepting bribes and were sentenced to prison terms of between seven and 14 years. The Shanghai trial of the four was conducted in secret.


Originally, the Rio Tinto employees had been charged with stealing state secrets, which could have resulted in death penalties.


“This all adds up to greater concerns for businesses that want to do business in China and still maintain standards of privacy of customer information and your own company information,” Boehme advises.

What can corporate boards do?

Michael Yip, a vice president in the risk consulting practice at Marsh USA, says in an e-mail that lately he's seen some boards require more reports on how security policies are being adhered to. Often that's in the form of metrics for compliance and effectiveness of identified controls.

In a recent Agenda survey of directors and executives, respondents said that among the three most important risk factors that their boards have to oversee this year are “flawed behavior in China and the Far East,” “foreign country regulatory risks,” and “cyber attack.”

 Espionage aside, says Kossovsky, the most common tool for IP theft is the Request for Information that a company sends to collect information

 about a supplier's capabilities. The best mitigant against that risk could be a policy on how much your company provides and to whom.