GOVERNANCE & ACCOUNTABILITY INSTITUTE'S
TO THE POINT™
Timely News, Insights & Perspectives on Corporate Sustainability, Responsibility & Citizenship

December 2017

Governance & Accountability Institute shares timely news, insights and perspectives with corporate managers in key topic areas:

- *Corporate Citizenship,*
- *Corporate Responsibility,*
- *Corporate Sustainability,*
- *Community Affairs, and*
- *Sustainable Investing.*

To the Point! is a fee-based educational resource for corporate executives and managers distributed each month with periodic brief updates for critical items.

Published by Governance & Accountability Institute, Inc.
New York, New York

Researchers, Consultants & Strategists

Tel 646.430.8230
Email info@ga-institute.com
Web www.ga-institute.com

IS YOUR COMPANY'S KEY DATA & "SECRET SAUCE" SAFE? Pssst! Foreign Entities Are Snooping…

A Management Brief - For Various Functions Within Your Company

Addressing the Risks for U.S. Companies — A Trio of Experts Look at China's Organized Cyber Espionage, and Impacts on Trade, Tech Transfer, Strategic Advantage…and Other Concerns for Multinationals

"Cybersecurity" is an important buzzword now among stakeholders — investors, customers, suppliers, regulators, media.

The recent crises events involving theft of critical information at **Equifax**, **HBO**, on the **UCLA** server, almost the entire body of Federal government employee records, **Target** retail customers records, and many others in the U.S.A. are raising questions about cyber safety and security. Companies are thinking about…

- How secure is my customers' information? May they be wondering about their own safety?
- What risks lurk in joint ventures, entering foreign markets with strings attached for "sharing" of processes and intellectual property, maybe R&D?
- What might the ripple effect be if my key suppliers' information is hacked, leaked, tampered with?
- What is the impact of a serious hack moving up and down my value chain?
- What about my company's *Intellectual Assets* — how safe are they? *They are the Keys to the Kingdom!*

CNBC said: Worldwide in September 2017 there were **918** data breaches compromising almost 2 billion records from January-to-June 2017. That is 164 percent above the same period in 2016.

And numerous governments have been reacting to the threat by introducing

legislation to force companies to disclose their data breaches. So who are the culprits prying into your server farm?

China and the United States — and Chinese Cyber Espionage

One of the frequently-accused players in corporate hacking and theft are various Chinese interests — private and state-owned companies; the military (especially **Peoples Liberation Army Unit 61398**, organized for digital spying); and, the central and provincial governments, which often require that western companies coming to China for marketing and other activities share certain elements of their secret sauce with China.

After a series of incidents of industrial spying on American companies by Chinese interests, in September 2015 the Chinese government agreed *not* to hack U.S. trade secrets to gain the edge and better compete with U.S. and western nations' companies.

The FireEye Inc. U.S. network security company told Reuters News in June 2016 that breaches attributed to China-based groups had plunged 90 percent over the past two years.

Before a bilateral agreement was reached, the Peoples Liberation Army unit was identified as the culprits behind a campaign of very well-organized economic espionage.

The targets included **U.S. Steel, Alcoa**, and **Westinghouse Electric**. Five PLA officials were indicted *(U.S. vs. Wang Dong)*; sanctions were threatened, and an agreement was reached during the **Obama Administration** that Chinese interests would not attempt to / or actually steal American corporate assets via digital espionage.

At the time we were studying a report by three experts on the structured, organized campaign inside China to conduct **Cyber Espionage**. We share highlights of that research and reporting effort with you.

Given the significant effort that goes into such "espionage," has the effort really stopped? Our conclusion was then, and is now, that U.S. firms should not let down their guard.

The 2013 Research Effort — China Cyber Espionage

Background:
China interests spying on U.S. business, financial, government and other strategic interests have been a point of tension

between the two countries since the early 2000s.

By 2010, "suspected" Chinese spying on American businesses and the government (agencies such as the **U.S. Department of Defense**) had become a more urgent public debate. "Intrusions of key networks," notes **The Diplomat** website, has become a steady topic of discussion.

It should be noted here that *both* governments accused each other of cyber spying and espionage (USA and China).

A new leader in China — **Premier Xi Jinping** — tried to create a new climate of cooperation in September 2015 by saying the Cold War had ended and the United States and China should be cooperating to reach "non-conflict, non-confrontational, mutual respect, and cooperation…"

> ***But had the Chinese cyber espionage really started to wind down? Are U.S. companies really safe from such snooping and theft of secret sauce of various kinds?***

The three experts looked at Chinese Industrial Espionage and shared their extensive research and wise perspectives in a book of that name. They are **Dr. William Hannas** (University of Pennsylvania), **Dr. James Mulvenon** (University of California and Defense Group Inc. and **Anna Puglisi** (visiting scholar Nankai University Department of Economics and a senior analyst in the Federal government).

Their Top Lines for Corporate Managers' Considerations

They explained: China espionage is fundamentally about a previously Third World country that systematically used technology provided by the world's leading economies (like the U.S.A.) to overtime achieve economic dominance and (the three authors think) could dominate strategically as well in the longer-term.

More recent China exports to the United States are manufactured goods of increasingly technical sophistication. Western technological resources are considered "to be transferred" to China as that country "sucked in" foreign proprietary achievements…" mostly off the books," they posit.

In the United States companies file the patents for IP protection while China interests build the products and pay royalties. *Ah,* in theory: China interests are imply not paying and "piracy" is rampant, the three experts argue.

These conditions that have persisted over years motivated the authors to write their book. They say:

- To alert decision-makers to the gravity of China technology transfer problem so that means are provided to address it.
- To raise awareness of the threat nationally; no amount of formal intervention will matter if the owners of the technology do not act on their own to protect it.

That means the companies in Silicon Valley especially.

China has a centuries-long tradition of sending their brightest to "learn from the West" and to return to lead China's steady march forward to greater development (such as in nuclear, space and missile programs).

The tradition is captured in **Zhang Zhidong's** 1878 "**Exhortation to Study**," a/k/a the **Quan Xue Pian** essay ("Keep China's style of learning to maintain the societal essence and adopt western learning for practical use – the principle of yi-tong.")

The authors describe the official "Science & Technology (S&T) exploitation" as an open source system.

Those who studied abroad brought know-how back to China, usually through such organizations as the **Beijing Document Service**, the **Institute of Scientific and Technical Information** and the **China Defense S&T Information Center.**

Through this system, scientific, technological, economic and higher education institutions get timely access to information to promote the development of science and technology *within* China. This system was put in place in the 1950s as the Communist government was creating their new nation.

"Open source" can mean such things as China interests getting more than half of their S&T intelligence from the reliable journals and periodicals of the west.

Does your key executives' information sit on an S&T database? Things like their biographical notes, work histories, nature of missions, leadership in organizations, financial circumstances, primary activities & duties, publishing of articles — the authors say this and much more sits in S&T databases.

And China mines the information for present and future use.

Within the Chinese military, there are departments set up to focus on foreign defense-related S&T (such as shipbuilding and electronics).

Content from the many conferences in the U.S. is collected, organized and shared within specialized units. So an aerospace conference content may yield critical information (including PowerPoints and videos) on laser weapons, radar, computer warfare, countermeasures, GPS systems, anti-stealth technology…and more.

Especially helpful information for key snoopers as they pry open the "treasury":

The U.S. Patent & Trademark Office treasure trove; the **Patents Section of the [China] CAS National Science Library** collects and analyzes patent literature, which over time became a major source of S&T intelligence for "local patrons".

Patent information from two dozen other nations are a valuable source as well, say the three experts.

Another important source of information is the "**Trade for Technology**" policy. The good news is that since 1978 China has been in a paradigm shift, moving from *concentration on production-for-export* to domestic *consumption-based-growth* (particularly for an emerging middle class in huge urban areas).

Important for Western companies: These policies include a shift from reliance on foreign business interests to domestic firms.

There is a perception — popular now in the U.S. media and opponents of liberal trade policies — that western companies are transferring critical intellectual properties to China in exchange for entry to the Chinese market.

The authors dispute *some* of this; they posit that critical-path **R&D** continues to be done in the western industrialized countries, with little technological innovation actually being done *inside* China (including product design) by foreign partners in joint ventures, for example.

The perception is that lack of effective intellectual property rights protection *is* harming western nations' companies *is* on target; the experts argue that lack of such protections has made foreign companies more wary of the threat.

"Local" R&D is concentrated in the information and communication technologies (by multinationals) in Beijing, Shanghai, Guangdong and several other cities.

The USA Lacks and Industrial Policy

One difference between China and the United States is the embrace of an agreed-to, formal ***industrial policy***; the Chinese government designates "champions".

The U.S. had a very robust public debate about this in the 1980s and moved away from the concept. Local industries were not officially protected (**tires, autos, steel, consumer electronics**) from foreign entrants to their markets. (The workers in those industries all too often saw their jobs disappear over the years.)

The authors identify the multinationals operating in the China R&D centers as including: **ABB, DoCoMo, Ericsson, Google, HP, IBM, Intel, Microsoft, Novo Nordisk, Cisco, Coca-Cola, DuPont, Eli Lily, Roche, Unilever**, and others.

Chinese public policy encourages the establishment of such labs.

To be kept in mind: **The China Ministry of Science and Technology** dedicates resources to the acquisition of foreign technology through a variety of programs.

Its mandate since the 1990s is quite sweeping, including postings of diplomats in key places around the world to guide the work of China nationals. The work is done through diplomatic offices; facilitation companies; ethnic Chinese professional organizations; university alumni organizations.

The government policies include establishment of "non-political" expatriate organizations that make them (in the authors' words) *de facto* agents of the Chinese government.

The liaison work is done through China government offices in New York, Chicago, Houston, San Francisco, Los Angeles; consulates in New York and San Francisco.

Important "connections" are established with U.S. universities, for example.

- One key organization in this effort identified by the authors is the **Chinese Association for Science and Technology, USA**. It had at the time of the study (2013) 11 chapters in 30 states; it serves as "a bridge" between China and the United States for cooperation in science and technology, economics, trade, and exchange of personnel and information exchanges.
- Another is **The Chinese American Professors and Professionals Network**, operating mainly in California (it was established back in 1991) to "high level" specialists in S&T.
- "**Scholars Net**" facilitates "rapid exchange" of information between scholars; members help set up meetings for Chinese experts with U.S. universities and R&D facilities.

A significant part of the authors' work involves the role of China's students in the United States. The early waves of students studying in the U.S. tended to stay in the U.S. While China could not provide the kinds of environments for graduates in the home country, the government sees the U.S. trained Chinese citizens as a *bridge* between the countries, with "two bases" in the massive *Diaspora* of the past three or more decades. They are expected to contribute to the social and economic advance of China in various ways.

The Players in Chinese Espionage

As for "traditional Chinese espionage," this is mainly the mission of: the **Ministry of State Security;** the **PLA's Military Intelligence Department;** the **People's Liberation Army's SIGINT Departmen**t.

All pose a long-term threat the United States, say the authors. And says the **Federal Bureau of Investigation** and other U.S. agencies.

The Chinese have a philosophical approach to this work. Success could be through "a thousand grains of sand"; the "mosaic" of information gathered; the "human wave" or "legions" of those helping; the "vacuum cleaner" approach; or pattern recognition.

Experts quoted say that China sends out literally thousands of people with limited tasking to flood foreign countries" to gather bits (of sand) — intelligence of some value.

One vexing issue that the authors describe is the "knowing" of the "who" of Chinese corporate ownership.

Who's Who

The U.S. Department of Defense apparently keeps a list of companies that are owned by the China military — there may be up to **3,000** government- and military-influenced companies operating within the United States of America.

A number of these have links back to China for gathering of intelligence, technology targeting, and acquisition roles.

And so we come to the critical nature of digital/cyber espionage.

Keep in mind, the authors' work was done in 2013 and so the challenges may have increased dramatically over the past four years.

They stated then:

"***Cyber espionage is the latest and perhaps the most devastating form of Chinese espionage, striking at the heart of U.S. military advantage and technological competitiveness***."

Quoting an American general, "***…cyber espionage represents the greatest transfer of wealth in history.***"

The strategic context of Chinese espionage is the use of cyber as an overt tool of state power.

Among the tools that U.S. and multinational managers should keep in mind as outlined by the authors:

- Foreign-focused anti-monopoly laws.
- Mandatory tech transfer.
- Compulsory technology licensing.
- Rigged Chinese standards & testing rules.
- Local content requirements.
- Mandates to reveal encryption codes.
- Excessive disclosure of scientific permits and tech patents.
- Discriminatory government procurement policies.
- Failure to enforce protection of intellectual property rights.

These are techniques *not* to destroy U.S. competitiveness, explained a head of the **FBI Counterintelligence Unit**, but to exploit systems for information advantage such as looking for the characteristics of a weapons system by a defense contractor or academic research on plasma physics…"

Strategic advantage thus can be achieved through hacking. The **U.S. State Department** and the **Department of Defense** are under constant attack, say intelligence experts.

Setting the Chinese cyber espionage in context, the authors offer these perspectives:

- The cyber-spying activities are a "collage," with interacting components. This includes use of open source software; peeking in on non-Chinese R&D taking place in China; technology transfer requirements that result in sharing of multinational secret sauce; the role of overseas students and graduates, and professionals; the work of various Chinese-sponsored organizations to gather information inside the United States; and, abuse of cyberspace.
- All industrialized nations are experiencing some form of the above within their borders.
- China often sees these activities as a "borrowing" and necessity for the development of the country. All too often, there is no penalty for China in pursuit of cyber espionage.

China Companies in the USA

Certain Chinese companies operating in the U.S. — such as **Huawei US/Futurewei** and **Haier** — are to be carefully watched, the experts said, as their products could be involved in spying or deliberate technology transfer that could damage the United States.

Indeed — the **U.S. Department of Defense / U.S. Cyber Command** in Fall 2015 blocked the use of telecom equipment produced by China's **Huawei Technologies** over fears of cyber snooping. The DoD leadership could not say whether key defense contractors may be using Huawei equipment.

Another risk for US defense contractors to watch if they are in the DoD supply chain.

> ***And then there are "American" companies owned by Chinese nationals that are focused on transferring technology back to China from the U.S.***

Some companies are described by the experts as "hybrids," operating as private companies but being provided loans, tax breaks and political advantage by the Chinese government. (One is described as having the largest gene sequencing capacity in the world.)

The advice for U.S. multinationals operating in China is to be careful. What about companies *not* operating in China – what is the risk or threat to them in the context of all of this?

# # #

G&A Institute Shared Perspectives

Theft of intellectual property including the hacking of systems and databases known or suspected to be of Chinese origin can have a dramatic impact on U.S. company reputations and market valuations.

The impact of a major hack could have significant ripple effects, up and down the value chain (consider the concerns of your customers, suppliers, partners, lenders, employees).

It pays to be a bit paranoid in this regard; while the rise of China in economic, political, statecraft and military terms is providing in various situations threats to U.S. hegemony and other forms of leadership, relations with China are of importance to American and multinational companies of other nations.

As **President Ronald Reagan** liked to say — "Trust but verify." Good advice for the 21st Century.

The threat can appear to be overblown ("fake news?"). In June 2016 **Reuters** news reported that the government of China appeared to be abiding by a September 2015 pledge to stop hacking American trade secrets (so said cyber security and government officials).

The China Foreign Ministry said: "We oppose and crack down on commercial cyber-espionage activity in all forms." The prior spying and hacking activities were said to have shifted to spying on Russia, the Middle East, Japan and South Korea.

For managers to keep in mind:

- In sustainability / responsibility and other reporting, many frameworks and standards have provisions for reporting on information security. American companies are required by the **Securities & Exchange Commission** to have board of director oversight of "risk and opportunity," and cyber certainly falls in this category.
- Keep these factors in mind when developing your company's responses to third party queries and when preparing your sustainability report.
- Many investors / investor coalitions are moving cyber issues to the top of their corporate engagement discussions and preparing proxy initiatives to require more due diligence and public disclosure of steps taken (to address and mitigate risk and seize opportunities). Watch for news about these initiatives in early 2018.
- The major independent service providers (for ESG analytics, data, ratings & rankings, scores, and other resources for portfolio management) are increasingly incorporating cyber issues in their analytic work. MSCI and Sustainalytics are examples.
- 

There are several cyber-security firms (such as FireEye Inc. and CrowdStrike) that can be monitored for up-to-date information that may affect your firm. For example, when aerospace and defense firms are being actively targeted; when retailers lose vital customer information…and other developments.

Recently, ***Barron's*** magazine had a commentary on cyber security failures. *Why*, author **Alex Eule** wondered, haven't share prices dropped at certain firms after disclosure of a breach, while other companies did experience a share impact?

Equifax share prices plunged after its data breach was disclosed. **Target** and **Home Depot** did have similar sell-offs. "For Corporate America, " Eule writes, "the lesson may be that disclosure is more important than the event."

He goes on to say that companies coming to market — such as **Uber** – should keep these lessons in mind. (Uber recently was hacked and was slow to disclose; it is still a privately-owned firm.)

It does seem to be that early disclosure of breach and hacking issues benefits the firm vs. "late" disclosures (sometimes coming months after the attack and loss of valuable assets).

Wall Street doesn't like surprises, as the old saying goes!

# # #

References For You

The content highlighted above is from an extensive, thoroughly researched and heavily footnoted work published in 2013 (ISBN 978-0-415-82142-1): *Chinese Industrial Espionage — Technology Acquisition and Modernizatio*n. Published by Asian Security Studies, Rutledge, Oxford, England. Rutledge is an imprint of Taylor & Francis Group.

The authors/editors of the study are William C. Hannas, James Mulvenon, and Anna B.Puglisi; they are Copyright owners.

Scholars and experts providing content included in the publisher's Asian series: Peter Horwath, Na Li, Dennis Blasko, Edwin O'Dowd, Martin Wayne, Rajesh Basrur, and others.

In January 2016, U.S. business leaders, government officials and security agencies appeared on a **CBS "60 Minutes"** segment that Chinese Cyber Espionage is a "National Security Emergency." Report:
https://gizmodo.com/justice-department-says-chinese-cyberespionage-is-a-nat-1753528044

You can see the broadcast here ("The Great Brain Robbery," reported by **Lesley Stahl**):
https://www.cbsnews.com/news/60-minutes-great-brain-robbery-china-cyber-espionage/

Alex Eule's column in Forbes (November 27 2017) was: "Uber, Come Clean."

# # #

November 28th 2017 News Update

Just as we finished this brief, ***Forbes*** reported on Chinese cyber espionage — it is long-standing and appears to be continuing. **Siemens** was attacked and allegedly lost 407 GBs of data. Three Chinese nationals were charged with stealing from **Moody's Analytics, Trimble** and Siemens; data and trade secrets were stolen.

Two of those indicted were founders of an organization (**Guangzhou Bo Yu Information Technology Company Limited,** or **"Boyusec"**) that is characterized as one of "the more advanced and active government-sponsored espionage groups." The company evidently works as a "cut out" (spy craft talk) for the official agencies of China that spy on other nations' companies and government agencies.

Note that Huawei was listed on the Boyusec web site as a partner (since wiped off the site).

Boyusec targets are companies in defense, aerospace, energy, telecommunications and advanced technologies. Traces of their work goes back to 2007. The pace of attacks, says **CrowdStrike**, has picked up since 2016 (and the agreement signed between the U.S.A. and China!).

Tribble was designing an accurate satellite navigation technology. Moody's had email compromised and switched to other accounts.

Forbes Link:
https://www.forbes.com/sites/thomasbrewster/2017/11/27/chinese-hackers-accused-of-siemens-moodys-trimble-hacks/#12885b7119ef