



PRIVACY UPDATE

U.S. Technologies and Trade Secrets at Risk in Cyberspace

In its report to Congress dated October 2011, “Foreign Spies Stealing U.S. Economic Secrets in Cyberspace,” the U.S. National Counterintelligence Executive (“NCIX”) provided harrowing details regarding the pervasive and growing threat of economic cyber-espionage being conducted against U.S. corporations.¹ Foreign perpetrators—identified in the report as emanating primarily from China and Russia—are described as targeting American companies to obtain sensitive intellectual property, technology data and other business secrets.

The new NCIX Report suggests that foreign actors will “remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace.” In addition to highlighting numerous disturbing examples of cyber-intrusions into corporate networks and information systems, the report provides extensive recommendations for enhancing corporate cybersecurity, and includes an action plan for “Best Practices in Data Protection Strategies and Due Diligence for Corporations.” Click [here](#) for outline.

Cyber-Risks

The NCIX Report indicates that: “economic espionage inflicts costs on companies that range from loss of unique intellectual property to outlays for remediation, but no reliable estimates of the monetary value of these costs exist. Many companies are unaware when their sensitive data is pilfered, and those that find out are often reluctant to report the loss, fearing potential damage to their reputation with investors, customers, and employees.”

Many of the internal controls and safeguards applicable under corporate privacy and data security programs for protecting personal information of consumers and employees are also, of course, relevant to protecting business assets against cyber-espionage. The risks and response are not entirely the same, however. Cyber-risks call for distinct consideration by boards of directors and company leadership as noted in the U.S. Securities and Exchange Commission’s recent guidance on cybersecurity risk disclosures.²

The NCIX Report sets forth its view of corporate duties to protect against cyber-attacks as follows:

“The private sector already has a fiduciary duty to account for corporate risk and the bottom-line effects of data breaches, economic espionage, and loss or degradation of services. A key responsibility of chief executive officers and boards of directors is to ensure that the protection of trade secrets and computer networks is an integral part of all corporate decisions and processes and that all managers—not just security and information

¹ See http://www.ncix.gov/publications/reports/fecie_all/index.html

² See <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>.

systems officials—have a stake in the outcome. Viewing network security and data protection as a business matter that has a significant impact on profitability will lead to more effective risk management and ensure that adequate resources are allocated to address cyber threats to companies.”

Specific Cyber-Risks Noted in NCIX Report

One of the more serious cyber-risks described in the Report involves computer network intrusions originating overseas, which private sector specialists typically call “advanced persistent threats.” Some of these reports have alleged a foreign government or government sponsor of the activity, but the U.S. intelligence community has not been able to attribute many of these private sector data breaches to a state sponsor.

The Reports states that such persistent foreign collectors will remain interested in all aspects of U.S. economic activity and technology, but the greatest interest is likely to concentrate on:

- Information and communications technology;
- Business information, including corporate transactions, that provides foreign actors an edge in negotiations with U.S. businesses or the U.S. Government;
- Military technologies, particularly marine systems, aerial vehicles, and other aerospace/aeronautic technologies; and
- Civilian and dual-use technologies in sectors likely to experience fast growth, such as clean energy and health care/pharmaceuticals.

The Report notes that even when a company knows its sensitive information has been stolen, that its computer networks have been penetrated, or that they have been compromised by a Wiki-leaks type insider, it may choose not to report the event to the FBI or other law enforcement agencies. The Report indicates that “no legal requirement to report a loss of sensitive information or a remote computer intrusion exists, and announcing a security breach of this kind could tarnish a company’s reputation and endanger its relationships with investors, bankers, suppliers, customers, and other stakeholders.”

Given the SEC’s recent cybersecurity guidance, federal and state data breach notification requirements, U.S. Department of Defense contractual provisions (including a pending rulemaking proposal), and cybersecurity legislation being considered in Congress, it is an oversimplification for the Report to state that there is “no legal requirement to report a loss of sensitive information or a remote computer intrusion.” Companies should evaluate their affirmative legal obligations very carefully to determine what if any reporting requirements are necessary or appropriate in connection with cyber-attacks, network intrusions or loss of sensitive data. Indeed, companies often require their service providers, business partners or other counter-parties to disclose any loss of transferred or shared proprietary information, trade secrets or other confidential data in contractual provisions.

The immediate prognosis is not necessarily encouraging. The Report concludes that “the globalization of the supply chain for new—and increasingly interconnected—IT products will offer more opportunities for malicious actors to compromise the integrity and security of these devices.”

NCIX Recommendations

The Government’s action plan referenced above, for conducting assessments and implementing safeguards, “Best Practices in Data Protection Strategies and Due Diligence for Corporations,” entails:

- Develop an “information strategy,” promoting effective data management and controls
 - Develop data protection policies
 - “Take stock of company data—not just in databases but also in e-mail messages, on individual computers, and as data objects in web portals; categorize and classify the data, and choose the most appropriate set of controls

and markings for each class of data; identify which data should be kept and for how long. Understand that it is impossible to protect everything.”

- Enhance internal awareness of risks and assess insider threats
- Increase attention to network security, auditing and monitoring
- Engage in contingency planning for compromises and intrusions
- Use government resources of NCIX and FBI to help develop effective data protection strategies

We believe that the NCIX Report would make very worthwhile reading for senior executive and board members for any company that relies on or has possession of significant information assets.

Cybersecurity Assessments

Sidley Austin LLP has previously reported on related cyber-risks and responsibilities in “Cybersecurity – It’s Not Just About ‘National Security’ Anymore: ‘Directors Desk’ and Other Incidents Sound Wake-Up Call for the Executive Suite and Board Room.”³ We believe that conducting internal cybersecurity as well as overall data protection assessments is appropriate for many companies to consider as part of their information governance internal controls.

Such assessment should consider the collection, use and movement of sensitive trade secrets and personal data within an organization and analyze the structures governing how the data is acquired, used, shared, and stored within an organization across its lifecycle. These assessments can be very useful in understanding how well an existing data protection program is actually working, and in demonstrating to regulators that data protection commitments are taken seriously and have been honored. Further information about Sidley’s Information Governance Assessment is available at www.Sidley.com/InfoLaw.

If you have any questions regarding this update, please contact the Sidley lawyer with whom you usually work.

The Privacy, Data Security & Information Law Practice of Sidley Austin LLP

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes regulatory compliance lawyers, litigators, financial institution practitioners, healthcare lawyers, EU specialists, IT licensing and marketing counsel, intellectual property, and white collar lawyers. Sidley provides services in the following areas:

- Privacy and Internet Litigation and Regulatory Advice
- Data Breach, Incident Response, and Cybersecurity Advice
- Global Data Protection and Information Security
- Information Governance Assessments and Compliance Programs
- International Data Transfer Solutions, Outsourcing and Cross-Border Issues
- Cyberlaw, E-Commerce, Social Media, Cloud Computing and Internet Issues
- EU, China and Japan Compliance Counseling
- Gramm-Leach-Bliley and Financial Privacy
- HIPAA and Healthcare Privacy
- Communications Law and Data Protection
- Workplace Privacy and Employee Monitoring
- Unfair Competition, Advertising and Consumer Protection
- Website Policies Online Trademarks and Domain Name Protection
- Records Retention, Electronic Discovery, Government Access and National Security

To receive future copies of this and other Sidley updates via email, please sign up at www.sidley.com/subscribe

³See <http://www.sidley.com/sidleyupdates/Detail.aspx?news=4747>.

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG LONDON LOS ANGELES NEW YORK
PALO ALTO SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.

www.sidley.com

Sidley Austin LLP, a Delaware limited liability partnership which operates at the firm's offices other than Chicago, London, Hong Kong, Singapore and Sydney, is affiliated with other partnerships, including Sidley Austin LLP, an Illinois limited liability partnership (Chicago); Sidley Austin LLP, a separate Delaware limited liability partnership (London); Sidley Austin LLP, a separate Delaware limited liability partnership (Singapore); Sidley Austin, a New York general partnership (Hong Kong); Sidley Austin, a Delaware general partnership of registered foreign lawyers restricted to practicing foreign law (Sydney); and Sidley Austin Nishikawa Foreign Law Joint Enterprise (Tokyo). The affiliated partnerships are referred to herein collectively as Sidley Austin, Sidley or the firm.

SIDLEY AUSTIN LLP
SIDLEY