VENABLE® LLP

Technology Transactions Alert

April 2013

Information Security Implications for Business Agreements

AUTHORS

Armand J. (A.J.) Zottola

Robert F. Parr

RELATED PRACTICES

Technology Transactions and Outsourcing

Corporate

ARCHIVES

2013 2009 2005

2012 2008 2004

2011 2007 2003

2010 2006

On February 12, 2013, President Obama signed an Executive Order ("Order") that outlined a voluntary cybersecurity framework ("Framework") designed to help protect the nation's critical infrastructure, which is generally defined as those systems or assets, whether physical or virtual, which are so vital to the United States that their incapacitation or destruction would harm public health or safety, economic security, or national security. The Department of Homeland Security has already designated the following 16 economic sectors as home to the U.S. critical infrastructure: information technology services, energy, telecommunications, banking and financial services, chemicals, manufacturing, transportation, emergency services, food and agriculture, healthcare and public health, the defense industrial base, government and commercial facilities, nuclear reactors, materials and waste, and water and wastewater systems. The Framework may therefore apply to countless companies of all sizes across a wide variety of critical infrastructure industries.

More generally, the Order has important implications for any private sector business because information security has rapidly become a hot button issue in this age of growing economic espionage, intellectual property and trade secret theft, and sensitivity to customer privacy. An increasing number of companies have recently reported data security breaches. Even a single security incident may lead to regulatory penalties, shareholder or customer class-action lawsuits, loss of customers to competitors, and irreparable damage to a company's brand or reputation. A company's best defense against any of these potential pitfalls is to take the steps necessary to sufficiently protect all proprietary and customer data.

Information Security Through Contract Drafting

Private sector businesses should now ensure that their agreements contain terms that effectively control access to and use and disclosure of their confidential or nonpublic intellectual property assets, such as patents, copyrights, and trade secrets ("Intangible Assets") and, separately, the personally identifiable information they store or otherwise retain ("Customer PII"). In an effort to minimize the likelihood of data breaches and the increasing number of data security obligations, businesses should even strive to consider safeguarding any Customer PII they are not presently obligated to protect under the patchwork of industry-specific privacy and information security laws, such as the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act. What follows is a list of suggested concepts that should be incorporated, as applicable, into business agreements with counterparties who may have access to Intangible Assets or Customer PII (collectively, "Company Information").

- ***Confidentiality.*** Establish permitted uses and disclosures of Company Information by service providers, contractors, subcontractors or other venders, or counterparties to transfer, sale, merger or acquisition transactions (together, "Business Counterparties"), and provide that such parties cannot use or further disclose Company Information except as permitted or required by the contract or law.
- ***Risk identification and assessment.*** Consider requiring Business Counterparties to use commercially reasonable efforts to (i) identify and assess reasonably foreseeable threats to the security of Company Information and the likelihood of harm and potential damage flowing from such threats; (ii) classify data according to type or sensitivity; and (iii) gauge the need to adjust security protocols to address new threats or handling and storage deficiencies.
- ***Safeguards.*** Provide that Business Counterparties must implement technical, administrative, and physical safeguards to prevent unauthorized access to or use or disclosure of Company Information. Examples of such safeguards include (i) compartmentalizing Company Information on a business-need-to-know basis; (ii) encrypting stored and transmitted Company Information; (iii) limiting access to Company Information through passwords, network firewalls, and locking up hardcopy records; (iv) auditing security protocols on a regular basis; and (v) requiring employee information security training.

- ***Incident response and breach notification.*** Require Business Counterparties to report any unauthorized access, use, or disclosure of Company Information within a specified time frame, and provide that they must follow baseline breach notification procedures, including (i) a prompt investigation into the compromised information by designated individuals or groups; (ii) obligations to report (or assist with reporting) breaches to required regulators and law enforcement authorities within a specified time frame; (iii) mitigation procedures designed to limit the dissemination of stolen Company Information; (iv) and obligations to promptly notify affected individuals under certain circumstances.
- ***Customer Privacy.*** Consider inclusion of provisions in privacy policies and agreements with customers which (i) explain the company's practices regarding the collection, use and disclosure of Customer PII in business transactions; (ii) give customers the right to control certain or all secondary uses of their PII, and to access and contest the accuracy of their PII; (iii) explain or reference the procedures designed to ensure the integrity and accuracy of Customer PII; and (iv) describe how customers may seek information.
- ***Restrictive Covenants.*** Require employees to sign enforceable nondisclosure or noncompete agreements to protect Intangible Assets and, in particular, Customer PII from being misappropriated upon resignation.
- ***Terms of Employment.*** Require employees to execute written agreements that establish clear policies regarding downloading Company Information onto external devices, the ownership and control of Company Information, including, without limitation, work-related social media accounts and Company Information loaded onto external devices, and the return or destruction of data upon resignation.
- ***Downstream obligations – subcontractors.*** Require a Business Counterparty to ensure that any subcontractor it may engage on its behalf that will have access to Company Information agrees to the same restrictions and conditions that apply to the Business Counterparty with respect to such information.
- ***Termination rights.*** Retain a right to terminate any contract with a Business Counterparty that violates a material term of its agreement relating to Company Information.
- ***Data access by Business Counterparties.*** Draft provisions that clearly describe the Business Counterparty's rights to access Company Information during the arrangement and, in particular, in the event of litigation.
- ***Data destruction or return.*** After contract termination, require Business Counterparties to return or destroy all data received from the company, or created by the Business Counterparty on behalf of the company.

If you have any questions, please contact the authors or a member of the **Corporate** or **Technology Transactions and Outsourcing Group**.