Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

5 Strategies For Avoiding Wiki Situations

Law360, New York (December 16, 2010) -- "Hacktivists," who recently launched attacks on banks, credit card companies and others, have served notice on American companies that governments are not the sole target of such digital disruptions. Days before his arrest on unrelated criminal charges in the U.K., WikiLeaks founder Julian Assange threatened to reveal confidential records of a major bank. While the United States government's countermeasures failed to prevent the release of sensitive classified information, there are five strategies for American companies to minimize the consequences of such attacks. With advance planning and immediate response, companies are not defenseless in the face of wiki warfare.

Kristen Mathews

First, companies should use available technology to minimize the risk of unauthorized data transfer. Data Loss Prevention (DLP) technology in corporate IT systems can be configured to prevent sensitive information from leaving corporate firewalls via e-mail, file transfer protocol, thumb drives and other portable media. Implementing digital rights management on highly sensitive documents makes them unreadable in the wrong hands.

Daniel B. Winslow

Companies also can develop a system of checks and balances for access to the most sensitive corporate information by requiring credentials of two separate personnel to access data. And newly patented technology will soon be available that requires both the physical presence of authorized personnel, as well as digital passwords, to aggregate and access confidential information from companies and their customers.

Second, companies need to include basic data security training for employees in their employment training and orientation programs. Training can range from basic, such as protocols for shredding documents and making shredders conveniently available to employees who handle sensitive documents, to more advanced training depending on an employee's access to data. Employees need to learn about "social engineering" techniques used by culprits to connive company personnel out of confidential information. Even commonly available social media sites such as Twitter and LinkedIn can pose sensitivity concerns if employees lack training in data and information integrity.

Third, companies need to revise internal and external contracts to strengthen legal protections against dissemination and misuse of proprietary data and corporate information assets. Employment contracts must include stern provisions prohibiting the unauthorized use or disclosure of data, coupled with significant liquidated damages and injunctive relief provisions that both act as a deterrent as well as an expedited form of legal remedy in the event of a breach.

Contracts with third parties in the supply chain need to include provisions to protect company trade-secret information in general so that immediate and credible trade secret claims can be asserted to retrieve legal control over information that has been compromised. A newly developed contract provision, the "Economical Litigation Agreement" or civil litigation prenup, can be included in business-to-business contracts instead of arbitration clauses to ensure that companies retain the

right to seek immediate injunctive relief in the civil justice system as well as to control the costs of any subsequent litigation.

Fourth, companies should consider copyrighting sensitive or propriety documents, to the extent possible, and asserting legal claims for injunctive relief in the event of a violation. In the event of an unauthorized use or disclosure of copyrighted information, the Digital Millennium Copyright Act enables companies to send a "take down" notice to the host of the website where sensitive materials are being published. Similarly, corporations can demand that servers and host sites enforce their acceptable use policies.

For example, PayPal terminated WikiLeaks' access, according to published comments by PayPal's general counsel, "Our actions in this matter are consistent with any account found to be in violation of our policies." And he explained that "we do not allow any organization to use our service if it encourages, promotes, facilitates or instructs others to engage in illegal activity." PayPal's rapid response to the apparent violation of its acceptable use policy is no small measure of the value of immediate enforcement of legal rights and options.

The fifth strategy for avoiding wiki situations involves minimizing damage in the event of a disclosure of sensitive or confidential corporate information. Companies should engage an online reputation management service vendor to immediately work to push down unflattering information on search engine results pages. Given the speed with which information transmits online, the better practice is to have such a vendor engaged or at least on call before any crisis arises. Reputation management may amount to closing the barn door after the horse gets loose, but at least the horse won't leave the barn at a full gallop.

Taken together, these strategies can help companies minimize the likelihood that sensitive data are released and diminish the consequences of any such release. The only certainty in digital data management is that prevention is the best medicine of all.

--By Kristen Mathews and Daniel B. Winslow, Proskauer Rose LLP

Kristen Mathews (kmathews@proskauer.com) is a partner with Proskauer in the firm's New York office and heads the firm's international privacy and data security practice. Daniel Winslow (dwinslow@proskauer.com) is senior counsel in Proskauer's Boston office, a former Massachusetts trial court judge and chief legal counsel to former governor Mitt Romney.