Susan Asam Quoted in *Crain's Detroit Business* Article on Global Cybersecurity

Offers Advice on How to Protect Trade Secrets and Customer Data When Dealing with International Business Partners Despite the Difficulty in Prosecuting Overseas Hackers

December 4, 2013

Susan Asam, an attorney in Dykema's Product and Professional Liability Litigation Group resident in the Firm's Detroit office, was interviewed for an article—"Biz Copes with Global Cybersecurity Complications"—that appeared in the December 1, 2013 issue of *Crain's Detroit Business*. The article focuses on the ever-increasing difficulties that U.S. companies face when endeavoring to protect intellectual property and consumer data from offshore hackers and cyberthieves.

Asam is a member of the ABA's Standing Committee on Law and National Security and the U.S. Chamber of Commerce's National Security Task Force, and has been involved in the implementation of Cybersecurity Executive Order 13636. She also co-authored the Dykema whitepaper, "Cybersecurity in the Private Sector: The Evolving Role of General Counsel," and helped plan the Firm's cybersecurity conference in September 2013, and has worked on a variety of matters involving cybersecurity and international transactions.

In the article, Asam comments on the stalled Cyber Intelligence Sharing and Protection Act (CISPA) legislation, which was re-introduced and passed by the U.S. House of Representatives in 2013, but stalled in the U.S. Senate. Asam observes that, even if new U.S. laws take effect, proper enforcement for overseas hackers will remain "a looming issue."

She notes that a key challenge facing multinational companies is jurisdictional cooperation. As countries are "sovereign states, you can't force U.S. law abroad." Asam adds that the recent episode in which a U.S. National Security Agency contractor (Edward Snowden) leaked government secrets has added new complexity to the issue.

"(Snowden) has definitely been a huge issue in all of this," Asam says. "Companies aren't going to share all their information with the government and trust it won't be disseminated beyond that."

Asam also offered several tips to help companies protect their trade secrets and customer information stored and transferred electronically, particularly when their business involves sharing these critical information assets to vendors and supply chain partners. Among the advice offered: the need for contracts to include cybersecurity provisions (such as cyber audit rights and indemnification clauses in the event customer information is hacked and/or compromised), the necessity of including cybersecurity on due diligence checklists for merger and acquisition transactions, and the importance of interviewing a business partner's technology team to understand fully their cybersecurity protections and breach response plan.

To read this article in its entirety, click here.

Practice Areas

Business & Commercial

Litigation

Product Liability