



Cyber-Attack

January 28, 2013

Imagine the power grid shutdown, transportation at a standstill, and a contaminated water supply all occurring at once. These collective disasters Janet Napolitano, United States Homeland Security Secretary, cautioned, could result from a major cyber-attack. Napolitano noted that such an attack could have a tremendous impact equivalent to Superstorm Sandy that crippled the Northeast. Napolitano referred to the impending threat as a “cyber 9/11”, stating that the nation’s infrastructure is left vulnerable to a potentially devastating attack. For instance, banks have recently fallen victim to a variety of cyber-attacks including disabled websites and infiltration by hackers. The plight of these banks serves to demonstrate a real and growing concern over the nation’s cybersecurity.

Napolitano pressed Congress to pass legislation enabling information-sharing between the private sector and the government. This type of cybersecurity will help safeguard the nation’s infrastructure that is predominately privately owned. However, previously proposed legislation has been met with significant resistance largely due to opposition by business and privacy groups. For instance, a bill that failed in Congress was aimed at increasing the flow of information between intelligence agencies and private companies but claims of governmental overreach and internet eavesdropping served to stifle efforts.

Napolitano is not alone in her quest to strengthen cybersecurity and prevent future attacks. Leon Panetta, Defense Secretary, expressed his concerns in a policy speech issued last October. Panetta cited increasing cyber threats that could “paralyze the nation.” In describing the potentially disastrous effects Panetta noted that possible targets include computer control systems operating water, electricity, and chemical plants as well as transportation systems. For instance, gaining access to a control switch would allow an extremist group to derail a train loaded with innocent passengers or hazardous chemicals. Panetta also emphasized the importance of cooperation between the military, government and private sector to ensure that the nation’s infrastructure is adequately protected. Also former Senator Joseph Lieberman was working on getting the senate to pass a watered-down version of what has been referred to as an “internet kill switch” which would have given the President enormous power over private networks in the event of a national cyber emergency. New legislation is being considered but its prospects of making it through Congress remain unclear. It is also anticipated that President Obama will issue an executive order setting up a voluntary system aimed at protecting critical infrastructure and incentivizing companies to contribute.

If you or your company has any questions or concerns regarding e-discovery, contact James G. Ryan at jryan@cullenanddykman.com or via his direct line at 516-357-3750.

A special thanks to Cynthia Thomas, a law clerk at Cullen and Dykman, for help with this post.