Is a Company Liable for Software Defects, when a Vulnerability is Discovered but Not Exploited?

If you are in the software business, you likely recognize that you can be sued for materially breaching contracts, infringing third party IP, and data breaches but you may not realize the extent of your liability just for making the sale of a software product deemed to contain a security flaw in the first place, even if the security flaw was never exploited and only identified.

Increasingly, however, just the act of selling software later deemed to be "defective" due to security flaws has resulted in liability to companies.

The Federal Trade Commision (the "FTC") has recently imposed fines and put in place ongoing oversight on companies for this type of issue.

But as Cisco just discovered, if the sales were made to a federal or state agency, the mere act of making the sale can also result in significant liability. Cisco has agreed to pay $8.5 million to settle a case originally filed in New York Western District Court in 2011 involving the sale of video surveillance technology to a variety of government organizations, including but not limited to Homeland Security, the Secret Service, the Army, the Navy, the Marines, the Air Force and the Federal Emergency Management Agency.

According to **The New York Times**, the Cisco case was initiated by the Justice Department in the Federal District Court for the Western District of New York, and the allegations were based on violations of the False Claims Act, which addresses

fraud and misconduct in federal government contracts. Fifteen states and the District of Columbia joined in the suit. As **The New York Times** reported, the argument made by the government was that the software had no value because if failed to serve its primary purpose of security enhancement. According to **The New York Times**, the flaw was identified back in 2008 by a Cisco subcontractor, who brought it to the company's attention at that time. However, as **The New York Times** reported, the subcontractor was subsequently terminated, and when he realized two years later that the vulnerability was still not fixed, he contacted the FBI. **The New York Times** reported that Cisco continued to sell the software with the flaw until July 2013, when if finally notified customers and fixed the flaw.

While the Cisco case applies only to sales made to government, a class action suit is pending right now on similar facts, where the sales were made to non-government consumers. The class action lawsuit was initiated late last year against Symantec for critical defects in its security products under the Norton Brand. It is not clear as to the status of that litigation.

The bottom line: if you are selling software that provides security functionality, you need to have internal systems in place to identify security flaws and quickly fix the flaws, particularly if the software is being sold to a government organization. However, if you are selling to the general public, you may still be liable for sales of the software containing security flaws, whether liability is assessed through the FTC or through class action litigation, regardless of the terms of your contract for those sales.