FTC Chair Threatens Action On Ransomware Holes

By Cara Salvatore
Law360, New York (September 8, 2016, 4:06 PM ET) -- Businesses could face trouble with the Federal Trade Commission if they fail to fix security holes that allow ransomware attacks, Chairwoman Edith Ramirez said Wednesday, threatening to continue a streak of now over 60 enforcement actions against companies with poor data security.

Speaking at a ransomware workshop assembled by the agency, the chairwoman said that companies that leave data vulnerable to ransomware — malware that lets hackers encrypt a computer's data and hold it hostage until payment is extracted — may be running afoul of the law.

“A company’s unreasonable failure to patch vulnerabilities known to be exploited by ransomware might violate the FTC Act,” Ramirez said. She cited the example of ASUS, a computer maker, whose “pervasive security bugs left the company’s routers vulnerable to malware, and that attackers exploited these vulnerabilities to reconfigure consumers’ security settings and take control of consumers’ web activity,” as alleged in a recent FTC action against the company.

The threat of ransomware has ballooned. There have been an average of 4,000 ransomware attacks per day in 2016, a 300 percent increase over the 1,000 ransomware attacks per day in 2015, according to the Department of Health and Human Services, which relied on FBI data.

Chairwoman Ramirez told the conference, “No one is immune — individual consumers, government agencies, and entities of all types and sizes have been targets.”

A data ransomer's demand is usually $500 to $1,000, Ramirez said, but can be as high as $30,000. Hollywood Presbyterian Medical Center in

Southern California paid a $17,000 ransom after an attack that “crippled” its systems and left doctors logging patient information “with pen and paper.”

The half-day workshop was intended to educate participants on what preventive steps they should take, what law enforcement has learned in fighting ransomware, and whether ransoms should be paid, the chair said.

It included three panels with participants from PricewaterhouseCoopers and Symantec as well as FTC Chief Technologist Lorrie Cranor, who is on leave from Carnegie Mellon University for the secondment.

In July, the U.S. Department of Health and Human Services said that ransomware attacks against a health facility or provider will generally be considered a breach of personal information under the Health Information Portability and Accountability Act.

Jocelyn Samuels, director of HHS' Office for Civil Rights, said the nature of a ransomware attack fits the criteria to label it a data breach.

“When electronic protected health information is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a 'disclosure' not permitted under the HIPAA Privacy Rule," the guidance report said. "Unless the covered entity or business associate can demonstrate that there is a '… low probability that the PHI has been compromised,' ... a breach of PHI is presumed to have occurred.”

Meanwhile, in March, Chairwoman Ramirez said the rapid growth in the so-called Internet of Things has also significantly increased risks to consumer privacy and safety and that companies are dawdling in addressing the risks.

The Internet of Things, or IOT, is “clearly still in its early stages,” but IOT devices have increased both in number and in sophistication, Ramirez told an American Bar Association IOT conference in Washington, D.C.

So companies need to take more steps to deal with the “significantly magnified” risks that this rapid uptake entails, maximizing the potential of the technology while still protecting privacy and ensuring consumer confidence, she said.

--Additional reporting by Jeff Overley and Daniel Wilson. Editing by Bruce Goldman.