Cybersecurity Standards Apply to Thee, Not Me

By: J.P. McGuire Boyd, Jr. & Robert Van Arnam

06.30.2015

?If there is anyone to blame, it is the perpetrators,? said Katherine Archuleta, Director of the federal Office of Personnel Management (?OPM?), to a Senate panel investigating the causes of the recent OPM cyberattack. During a separate hearing, Archuleta defended OPM?s failure to encrypt its data, explaining that encryption was ?not feasible to implement? on its legacy systems. Separately, Dr. Andy Ozment, Assistant Secretary for Cybersecurity at the Department of Homeland Security, explained that encryption would not have helped anyway because the hackers had valid user credentials and the OPM systems lacked multifactor authentication.

When it comes to cybersecurity, the federal government sets considerably higher standards for the private sector than it does for itself. The Federal Trade Commission (?FTC?), for example, views a company?s inadequate protection of consumer data as an unfair practice under section 5 of the FTC Act, 15 U.S.C. § 45. In 2005, the FTC charged BJ?s Wholesale Club with unfair practices after hackers stole customer information, alleging that BJ?s had acted unreasonably by failing to encrypt its data, among other shortcomings. By 2014, the FTC had settled 50 data security cases. *See* **here**.

The FTC?s pending action against Wyndham Worldwide Corporation illustrates the disparity in standards applied to the federal government versus the private sector. The FTC sued Wyndham in 2012 for failing to implement reasonable and appropriate cybersecurity measures in violation of the FTC Act?s prohibition against unfair acts or practices. According to the FTC, Wyndham left customer data unprotected by firewalls, did not encrypt credit card information, and used outdated software, among other lapses.

Following an unsuccessful motion to dismiss the unfairness claim, Wyndham appealed to the Third Circuit Court of Appeals on the question of whether a company?s failure to take reasonable cybersecurity measures constitutes an unfair practice under section 5 of the FTC Act in the absence of clear rules on exactly what constitutes reasonable and appropriate cybersecurity practices. The Third Circuit?s answer to this question, expected later this summer, should provide businesses with a better understanding of the cybersecurity standards to which they are held. Until the Third Circuit rules and

provides more clarity, companies should continue to look to guidance from the U.S. Department of Commerce?s National Institute of Standards and Technology available **here**.

Related People

- J.P. McGuire Boyd, Jr. ? 804.420.6927 ? mboyd@williamsmullen.com
- Robert Van Arnam ? 919.981.4055 ? rvanarnam@williamsmullen.com

Related Services

- Intellectual Property
- Intellectual Property Litigation
- Data Protection & Cybersecurity