The Government Can Sue Your Company for Negligent Cybersecurity

by Christopher B. Hopkins

While the risk of hackers dawned on many corporate lawyers after Target's data breach in 2013, the federal government has been actively suing corporations into cybersecurity compliance since 2005. Specifically, the Federal Trade Commission (FTC) has sued more than 50 companies for poor cybersecurity despite the lack of any specific statute on point. Even the Federal Communications Commission (FCC) has sued regulated companies for their lackluster data standards. It is not just credit card or health care data which needs to be protected, as evidenced by the recent Ashley Madison hack. All corporations need to be aware that they can be sued by injured parties (see the Seventh Circuit's *Remijas v. Neiman Marcus* opinion) as well as the federal government for what is best described as "negligent cybersecurity." The recent Third Circuit opinion in *FTC v. Wyndham* gives guidance on data practices to follow or avoid.

In April 2008, hackers broke into a Phoenix-area hotel's network and then connected to Wyndham's larger network. Using pure guesswork, the hackers paired usernames with frequently-used passwords as a brute-force method to break in. From there, hackers discovered unencrypted payment information and that Wyndam's system was practically unmonitored. Hackers repeatedly breached Wyndham's system and installed memory-scraping malware, resulting in $10 million dollars in fraudulent charges.

The FTC brought suit against Wyndham based upon Section 5 of the Federal Trade Commission Act which prohibits "unfair or deceptive acts or practices in or affecting commerce." Dating back nearly 100 years, Congress has intentionally kept the phrase "unfair practices" vague since, as one court wrote, "there were too many unfair practices to define." The FTC has determined that, under Section 5, it is "unfair" for corporations not to provide cybersecurity and it is "deceptive" for companies to have privacy policies which they do not follow. The FTC has brought suit against companies, alleging violations of the "unfairness" or "deceptive" clauses of Section 5, even when a company has not violated other statutes -- in other words, as one commenter wrote, the federal government has taken a "common law" approach to define negligent cybersecurity.

For a practice to be actionable as "unfair" under Section 5, it must be substantial; not be outweighed by consumer benefits or healthy competition that the practice produces; and it must be an injury that consumers could not have reasonably avoided. As the Third Circuit concluded, "[a] company does not act equitably when it publishes a privacy policy to attract customers…, fails to make good on that promise by investing inadequate resources in cybersecurity, and exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business."

In *Wyndham*, the defendant was sued for failing to take these steps:

- Use firewalls at critical network points;
- Restrict access to certain IP addresses;
- Use encryption for certain customer files (not plain text);
- Monitor network for previously-discovered malware;
- Employ common protection which prevents users from selecting weak passwords;
- Employ reasonable methods to detect and prevent unauthorized access.

Along these lines, in 2007, the FTC published a guidebook, *Protecting Personal Information: A Guide for Business*, which provides these recommendations:

- Check software vendors' sites regularly for patches and alerts about new vulnerabilities;
- Set firewall controls to limit access only to trusted employees with a legitimate business purpose;
- Require employees to use strong passwords;
- Implement a data breach response plan which includes immediate investigation and steps to close off vulnerabilities.

Until the *Wyndham* case, most companies settled with the FTC which limited the amount of attention paid to the FTC's "common law" cybersecurity negligence suits. Post-*Wyndham*, however, companies should be on notice of the risk of government suits; corporate counsel should review government settlement agreements online to ascertain what data compliance steps are considered adequate as a guide for developing a preventative plan. For this to work, legal and IT departments must collaborate. In the July 2015 settlement of *In re TerraCom, Inc. and YourTel America*, the FCC required:

- designating a senior corporate manager as a certified privacy professional;
- conducting a privacy risk assessment;
- implementing a written information security program;
- maintaining oversight of vendors;
- implementing a data breach response plan;
- providing privacy and security awareness training.

In light of *Wyndham*, companies (including law firms) should be on notice that, even in the absence of specific federal statutes, there is governmental and third party liability for poor data protection. In addition to following state statutes like the Florida Information Protection Act of 2014, recent FTC and other government agency actions and settlements should guide the development of cybersecurity protocols.

Christopher B. Hopkins is a member with McDonald Hopkins LLC. Send your data breach and privacy questions to chopkins@mcdonaldhopkins.com.