CARLTON FIELDS

# A Modern Game of Hide and Go Seek? Some Lessons Learned Following Sony and Other Widely-Publicized Data Breaches

March 25, 2015

While the recent hack of Sony was prominent news because of the celebrity ties and potential geo-political implications, other prominent cyber-attacks over the last few months are enough to give any company pause. The January 2015 hacks of Swiss bank BCGE and American health insurer Anthem show us, once again, that any company could be next. There is always the risk that an inside job could lead to the unauthorized disclosure of private, proprietary, and/or highly confidential information, including personal health information—any of which may result in lost business, reputational harm, regulatory actions, and/or civil lawsuits, such as the class action lawsuit filed in January 2015 against Sony Pictures by former employees alleging violations of the California Confidentiality in Medical Information Act. Sony succeeded in getting a good portion of its hacked material (e.g., movie scripts) removed from various websites—but this was primarily because the hacked material is protected under U.S. copyright laws, and thus was promptly removed by the websites pursuant to the take-down provisions of the Digital Millennium Copyright Act (DMCA). What other laws might be of use to a company following a data security breach, especially when the information does not fall under the DMCA? Consider the following federal statutes:

- Computer Fraud and Abuse Act (CFAA): The CFAA broadly prohibits unauthorized systems access, including by employees that exceed their authorized access. It provides for civil and criminal liability; however, a civil action requires a showing that the violation caused "loss" (as defined in the CFAA) aggregating at least $5,000 in value.

- Electronic Communications Privacy Act (ECPA): The ECPA provides for civil and criminal liability for unauthorized systems access, including any electronic communications (*e.g.*, emails) disseminated after such access, and allows for compensatory, statutory, and punitive damages, and reasonable attorneys' fees and costs.

- Stored Communications Act (SCA) of the ECPA: Under the SCA, it is a crime to intentionally access emails or other electronically stored communications without authorization, or to intentionally exceed authorized access to such communications. In a civil action, the SCA provides for compensatory, statutory, and punitive damages, and reasonable attorney's fee and costs.

**In addition, state computer crime and state trade secret statutes could afford protection and relief to companies that experience a data security breach.** However, in an increasingly interconnected world, it is possible that the laws of more than one state would be applicable in a particular instance. One fact remains true: being proactive before any data security breach is the best protection for limiting repercussions following a data security breach. This includes the implementation of a comprehensive written information security plan that outlines the necessary steps and contacts for recovering and limiting the spread of accessed information, and pursuing hackers, as well as frequently testing the plan for opportunities to improve its effectiveness.

## Related Practices

Technology
Intellectual Property
Cybersecurity and Privacy

## Related Industries

Technology