Cooley

January 14, 2015

Recent widely publicized cyberattacks have made clear that nation-state hackers are now hacking companies for political purposes and they appear to be focused on broadcasters and other media companies.

For example, last week, self-proclaimed Pro-Islamic State (ISIS) hackers calling themselves Cyber Caliphate infiltrated social media accounts of various media outlets. The group hijacked the website and Twitter account of a Maryland TV station for nearly two days, displaying ISIS propaganda on the station's website. The group launched a similar attack on the Albuquerque Journal, using the paper's Twitter account to display a profile picture supporting Islamic militants and other sensationalist posts. The breaches included what appears to be personal information about area residents and warnings that their confidential information is at risk. This marks the second time in two weeks that the newspaper has been hacked by Islamic State extremists.

Attacks such as these are not likely to stop, as evidenced by Cyber Caliphate's more recent attack on U.S. CENTCOM. Cyber Caliphate wrote on its Facebook page "You'll see no mercy infidels. We are already here, we are in your PCs, in each house, in each office…We hacked FBI databases. We won't stop…We know all your personal data: where you live, what you eat, your diseases, and even your health insurance cards." While their true affiliation is unknown, targeting these social media accounts to spread personal and/or sensitive information would signal a new tactic for ISIS.

These types of attacks are occurring more frequently against media companies. The FBI reports that "similar [cyber]attacks have been quietly happening to media companies across the United States." Media companies should consider ensuring that proper controls are in place to protect their social media accounts in addition to their network accounts and other confidential information. Remediation plans should also be in place to ensure that, if an attack occurs, the company can swiftly respond before too much damage is done.

These attacks are occurring at a time when the Federal Trade Commission and the Federal Communications Commission are increasing their vigilance over data security. For example, although the FCC took no action against broadcast stations following the infamous 2013 "Zombie Attack"—when hackers infiltrated emergency alert equipment to broadcast a fake Zombie invasion—the FCC has made it clear that it expects entities under its jurisdiction to take reasonable steps to protect data. Most recently, **the FCC fined two telecommunications carriers** $10 million for failing to take basic precautions to protect sensitive customer information.

The attorneys in Cooley's **Telecommunications** and **Privacy & Data Protection** practices work with a wide variety of media and telecommunications companies. We have substantial experience leading incident response efforts and advising entities that have experienced data breaches or other data security incidents. If you would be interested in learning more about our team and the collaborative approach we take in developing solutions to our clients' data security objectives, please let us know.

Principles, may be considered Attorney Advertising and is subject to our **legal notices**.

Key Contacts

Adam Ruttenberg Washington, DC	aruttenberg@cooley.com +1 202 842 7804
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090