Emily Westridge Black in Texas Lawyer: 3 Things GCs Should Know About Data Privacy Class Actions

August 2, 2016

PRACTICES Privacy and Cybersecurity, Litigation

Data breaches remain a huge concern for companies. So far this year, retailers including Wendy's, Omni Hotels & Resorts and Noodles & Company have informed customers that their personal information was compromised. Ironically, even Verizon Enterprise Solutions, which helps businesses and government agencies worldwide respond to data breaches, was recently hit by hackers who stole the information of about 1.5 million customers.

It's no wonder that in a March 2016 survey conducted by Consero Group in partnership with AegisAdvantage, cybersecurity topped senior legal executives' main areas of risk, with 52 percent of respondents naming it a major risk, followed closely by data privacy at 50 percent.

Just as data breaches are here to stay, so are the class action lawsuits that inevitably follow a breach. "If there is a breach of your company, you have to anticipate that there's going to be litigation," says Emily Westridge Black, an associate in the Austin office of Haynes Boone...

An example, Black says, are so-called breach-of-contract exclusions, which may be invoked by the carrier when a customer sues based on an alleged breach of contract of personal information, and the carrier argues that the insured held the information under a service contract. Another excluded area, she says, are "acts of foreign enemies."

"The problem here is that a lot of hacking is done by governmental or quasi-governmental entities abroad, particularly Russia or China," Black says. "While we haven't seen litigation about that, there could be circumstances where you have a cyberattack by the Chinese military, and you'll try and get coverage for that, but the insurance company can argue that that's an act of war or terrorism."

Excerpted from *Texas Lawyer*. To read the full article, please click here.