Published on *The National Law Review* https://natlawreview.com

Privacy Monday – June 22, 2015

Article By:

Cynthia J. Larose

The first Privacy Monday of the summer!

It's appropriate that the "boys of summer" feature prominently in today's post.

Strike three for the St. Louis Cardinals?

In 2014, news hit of a reported hack into the Houston Astros' vaunted "Ground Control" database and GM Jeff Luhnow said he intended to prosecute whoever was responsible. Last week's New York Times reported that it was likely Luhnow's old team, the St. Louis Cardinals. Reportedly, the Astros contacted the FBI when confidential information stored in the "Ground Control" database was posted online last year. Investigators found information indicating the origin of the hack was the home of a Cardinals' employee.

The most recent reporting on this story comes from CBS Sports, with an interview with Cardinals' owner Bill DeWitt and the report of a potential third violation of the Astros' database, purportedly by Cardinals' employees.

Recommended reading into the background of why the Cards would have bothered to hack the Astros can be found at ESPN: Why the Astros' sophisticated database would be worth hacking

Data Security Breach Documents Sought in Home Depot Books-and-Records Suit

Home Depot was recently hit with a books-and-records suit in the Delaware Court of Chancery, ***Frohman v. Home Depot***, which seeks documents relating to the giant retailer's data security breach last September. The plaintiff is requesting information concerning how the company first learned of the breach, any analysis of how the breach occurred, and what steps it took thereafter, among other topics.

The suit was brought under Section 220 of the Delaware General Corporation Law, which permits shareholders to request corporate documents for a "proper purpose." A proper purpose may include investigation of alleged wrongdoing by corporate officers and directors, if the allegations are adequately supported. The Delaware Court of Chancery has long encouraged shareholder plaintiffs

to use Section 220 to investigate their claims before launching a derivative suit alleging breaches of fiduciary duty by the board or management, and increasingly plaintiffs' attorneys have been following this advice.

Corporations that have been struck by data security breaches should anticipate that they may have to respond to such "books-and-records" suits seeking documents relating to the breach. Any corporate documents concerning the circumstances of a data security breach, subsequent investigations, and steps taken to prevent or remedy such breaches should be prepared with the awareness that these documents may well be requested in a subsequent shareholder suit. While it may be possible to limit access to these documents if they contain confidential commercial information or are protected by the attorney-client privilege and the attorney work product doctrine, the potential for disclosure should not be ignored.

Ten Essential Cybersecurity Questions to Ask Your CISO

Non-IT members of management typically struggle with how to determine what it is that they do not know, or what they should know, about their organizations' security profile.

IT Governance has posted a list of ten essential questions, including Are we conducting comprehensive and regular information security risk assessments?

National Law Review, Volume V, Number 173