New York Law Journal

White-Collar Crime

WWW.NYLJ.COM

An ALM Publication

VOLUME 256—NO. 60

MONDAY, SEPTEMBER 26, 2016

Of Redbirds and Rockets:

Corporate Espionage and America's Pastime

BY ANDREW GARBARINO

RAFAL PYTEL, ISTOCK

With the baseball season about to enter the post-season, perhaps it's time to revisit an interesting off-the-field legal drama from the 2015 season, namely the corporate espionage case involving two former National League Central rivals.

As originally reported in the New York Times,[1] the St. Louis Cardinals made news in connection with the alleged hacking of a database owned by the Houston Astros. The attack appears to have been in furtherance of a variety of potential motives: A desire to obtain intelligence from the Astros proprietary "Ground Control" database, to embarrass Jeff Luhnow, a former Cardinals executive who is now the Astros General Manager, or to determine whether Luhnow took data or other intellectual property developed by the Cardinals with him to a competitor. The FBI conducted an investigation into the allegations.

In December 2015, as a result of the FBI's investigation, Christopher Correa, then-scouting director for the Cardinals, was charged in a five-count indictment for his illegal access of Ground Control. In January 2016, he pled guilty to Unauthorized Access to a Protected Computer in connection with the illegal accessing of the Ground Control database. He was sentenced on July 18, 2016 to 46 months in federal prison and was ordered to pay $279,038 in restitution.[2] Prosecutors alleged that Correa caused approximately $1.7 million in loss to the Astros.[3]

Let that sink in for a moment. A Major League Baseball team was investigated by federal authorities for cybercrimes allegedly committed against another baseball team. And someone will be going to jail for nearly four years as a result.

The background of the matter is fascinating. While he was with the Cardinals, Luhnow developed a database called "Redbird". The

ANDREW GARBARINO *is of counsel with Ruskin Moscou Faltischek, where he is a member of the health care, white-collar crime & investigations and cybersecurity groups. Law student* COREY MORGENSTERN *contributed to the article.*

database was devoted in large part to advanced baseball analytics and, through the use of statistical information that was run through it, the Cardinals had great success in baseball's amateur draft, which culminated (after Luhnow left for the Astros,) with a World Series championship in 2013, at which time more than half of the 25-man-roster was comprised of players Luhnow played a role in drafting and developing, presumably by way of the statistical analysis provided in part by the Redbird database.

Despite the success he enjoyed in St. Louis, Luhnow left the Cardinals on less than cordial terms. Moreover, when Luhnow left for the Astros, he brought several other Cardinal employees along with him and developed the Ground Control database, which apparently shares similarities with the Cardinal's Redbird system. There has also been some talk that Luhnow or other former Cardinal employees may have logged on to the Redbird system after leaving the Cardinals. They may have simply logged in, if the Cardinals failed to delete old passwords or otherwise restrict access to Redbird.

Lost in the various news reports about the incident is the fact that the two organizations are billion-dollar companies working in a multi-billion-dollar industry. As with any business, the ability to access data and creative thinking developed and used by competitors is tantalizing—especially when only a discreet number of organizations operate within the sport.[4] Indeed, Major League Baseball teams employ a surprising number of employees, without even considering their minor league affiliates. In an industry like baseball, where staggeringly high dollar amounts are spent on the annual salaries of even mediocre players, the usefulness of large quantities of information cannot be overstated. When information has been developed by a significant competitor, the value of their closely-guarded information becomes almost incalculable from a competitive standpoint. The old saw that "information is power" is nowhere more starkly illustrated than in the talent-vetting of professional athletes.

While it may seem difficult to relate one's own work to the management of a sports team, the need to safeguard both data and proprietary information is germane to all businesses, regardless of industry. Protecting lists of vendors (and associated agreements and contractual terms), referral sources and communications are essential to the well-being of any company. That safeguarding of proprietary data doesn't even consider the vital need to protect customer or employee information, such as Social Security numbers and the like—always prime targets for computer-savvy interlopers.

Specialized industries—like baseball—present more specialized concerns, in addition to those described above. In health care, it could be guarding patient data in light of overwhelming regulation; in banking, credit information, account information and other important items at a time when hacking scandals are commonplace; in the mining industry, it could include data regarding prospective resource studies and geological surveys that a company spent significant resources obtaining. Indeed, no matter the industry, the failure to secure proprietary information, data and systems can be both devastating and embarrassing. Companies must actively consider what information held on their systems is most critical to their business and how to best protect that information.

The actual motivation aside, the "hack" in the Cardinals saga appears to have been accomplished by relatively low-tech means. Correa (and perhaps other Cardinals employees),[5] having access to prior passwords used by the employees who defected to the Astros may have simply tried those same or similar passwords in signing onto the Ground Control database.[6] Despite the $1.7 million figure stated by the government at the time of Correa's sentence, the true cost of the Astros failure to ensure the sanctity of the Ground Control data by not properly vetting passwords remains to be seen.

The monetary cost of cybersecurity is already reaching absurd heights and in this atmosphere of seemingly endless software updates and a constant influx of new products, it is easy to overlook or even disregard the risk of ensuring password security. Even then, those costs pale in comparison to the financial consequences of an actual data breach.

Password security requires a degree of effort that cannot simply be passed along to an IT group or tech vendor. The low-tech aspect of the attack is a useful lesson: Cybersecurity does not end upon software updates, the updating of hardware and devotion of time and resources to audits.

Rather, cybersecurity carries a major human resources component as well. The prevalence of remote access to company systems makes the sort of low-tech entry into a target's systems all the more dangerous, as the form of access itself will not trigger any alarm bells. These days, employee identification numbers or email addresses and a password are often all that is needed to access a workplace's network.

For that reason, it is critical to assess employee passwords on a regular basis. With new employees, they affirmatively should be asked whether they have used their password anywhere before. Better yet, they should be asked if they have even used a similar password in the past. For example, an employee using a password based upon his son's name and numeric birthdate, a password that has never been used by him in the past, will be dangerous if, at his previous employer, he used a password based on his daughter's name and numeric birthdate—it's just too easy to figure out for the sort of low-tech hacker, with access to former passwords. An explicit expression of the need for safeguarding company data should be a foremost concern with any new employee.

In the case of part-time employees, it goes without saying that an employee should provide assurances that they are using different passwords at their different jobs. In the case of vendors, confirming that any password-enabled access they are permitted is premised upon unique passwords should be mandated and in writing.

The continued sophistication and even cutting-edge methods of would-be hackers make the world of cybersecurity difficult enough. However, failing to recognize the low-tech or even no-tech aspects of password protection and rampant remote access can have far more damaging consequences, as the existence of a breach may go unnoticed for a significant amount of time. As in almost all business concerns, effective cybersecurity should start with effective communication to employees and vendors and not ignore obvious common sense considerations.

One of the first tasks upon the hiring of a new employee is to create an employee log-in. Regularly addressing the cybersecurity aspect of the new-hire process then, at an easy and natural moment, can avoid dooming the organization to costly audits and other consequences of a breach, like governmental scrutiny.

By carefully establishing and implementing workplace initiation policies that immediately address cybersecurity, the need to resort to and rely upon software safeguards and, worse yet, breach insurance coverage, may be avoided. Careful adherence to the human resources aspect of cybersecurity can only serve to strengthen overall security.

[1] Tyler Kepner, "Astors' G.M. Jeff Luhnow Delegates With a Drive for Data," THE NEW YORK TIMES (June 19, 2015), http://www.nytimes.com/2015/06/20/sports/baseball/cardinals-scandal-astros-jeff-luhnow-target-of-hacking-was-helped-and-hindered-by-technology.html?_r=0.

[2] "Christopher Correa, Former Cardinals Executive, Sentenced to Four Years for Hacking Astros' Database," THE NEW YORK TIMES (July 18, 2016), http://www.nytimes.com/2016/07/19/sports/baseball/christopher-correa-a-former-cardinals-executive-sentenced-to-four-years-for-hacking-astros-database.html.

[3] The loss was calculated in part by accounting for how the Cardinals altered their drafting based upon the information that was obtained from Ground Control.

[4] One need only look toward how quickly the Tom Brady/National Football League "deflategate" case progressed. Incredible amounts of money hinge on the performance of sports teams and athletes.

[5] Although only Correa was charged, news reports quote Cardinals officials as blaming the conduct on "roguish behavior by a handful of individuals."

[6] This report comes from the aforementioned Times article, though Astros executives have stated emphatically that all former Cardinal employee passwords were different than those previously used in St. Louis.