Foster Garvey

Sports & Entertainment Beat

Tips on Data Privacy after the Houston Astros Hack

06.17.15 01.07.26

The Department of Justice recently disclosed that the FBI and Justice Department prosecutors are investigating whether the St. Louis Cardinals hacked into the Houston Astros' computer network to steal information about the Astros' players. According to the New York Times, officials believe that "vengeful front-office employees for the Cardinals, hoping to wreak havoc on [former Cardinals executive and current Astros general manager] Jeff Luhnow ..." orchestrated the hack. The breach apparently occurred in 2013. The sports implications are interesting, but the data privacy implications are crucial. Specifically, the nearly nonexistent protection that the Astros allegedly afforded its valuable confidential information should give pause to any business that, without intensive verification, believes its information is safe.

Due to the Astros' lack of data privacy sophistication, discussed below, the hack apparently required minimal effort. While Luhnow was with the Cardinals, the team built a computer network, aptly called Redbird, to house its confidential information. When Luhnow left for Houston in December 2011, the Astros created a similar database, called Ground Control. Investigators suspect that Cardinals officials reviewed a list of passwords that Luhnow had used for Redbird, and used those same passwords to gain access to Ground Control. Apparently, the Astros learned of the hack when their information, such as internal trade talks, was published on the sports site Deadspin.

With this information, it is possible to catalogue mistakes the Astros organization may have made:

- Copycatting. Deliberately replicating a network used by your key competitor is practically begging for your competitor to exploit its knowledge of its own network to access your system. No one wants to reinvent the wheel, but at the very least, someone in the Astros organization should have ensured that the passwords had been changed. Businesses that employ people who move from one competitor to another need to take steps to ensure that their networks are not too technically similar to those of their competitors.

- Lack of Diligence. Many companies force their network users to change their passwords several times a year. The Astros is not one of those organizations. Remember, the Astros apparently established Ground Control - using Luhnow's passwords - when they hired Luhnow in 2011. Those passwords still worked in 2013, when the Cardinals allegedly hacked the system. In this day and age, retaining the same passwords for two years falls far short of best practices, to say the least.

- Inattention. This is the most critical error. Had the Astros engaged in an audit of their IT system to ensure that they were maintaining best practices, someone would have quickly caught the password duplication before it caused a problem. Additionally, if the Astros had implemented a data privacy protocol, they could have discovered the breach before they read about it on Deadspin. However, they were inattentive and complacent, and as a result, their competitor had unfettered access to their information.

The Cardinals could have also taken greater care with their own data security. The team maintained a database nearly identical to one they had reason to believe that their key competitor used. It was implemented for the Cardinals by Luhnow, so it was likely Luhnow would do the same for the Astros when he joined them. Had the databases been materially different - or perhaps even minimally different — the hack would not have worked. One can therefore easily imagine the hack working in reverse, with the Astros using their list of passwords to gain illicit access to the Cardinals' database. Is the only difference that the Cardinals had particularly "vengeful" employees? That is a thin reed upon which to rest your data security. Business that have reason to believe that their competitors are using their confidential IT information need to take steps to secure their network.

All this is to say that your mother was right. An ounce of prevention really is worth a pound of cure. And time spent implementing and maintaining an effective data security plan is guaranteed to pay off in the long run.

****

Sean C. Griffin is an Owner in Garvey Schubert Barer's Commercial Litigation and Data Information and Security Groups, working in its Washington, DC office.

Posted in Sports, Web/Media

Tagged as data privacy, Department of Justice, FBI, Houston Astros, Jeff Luhnow, St. Louis Cardinals