MELAND | BUDWICK

5 Questions In The Cardinals Hacking Scandal

https://mbdev.aplussdv.com/2015/07/20/5-questions-in-the-cardinals-hacking-scandal/

Zachary Zagger

News last month that the St. Louis Cardinals, a venerated baseball franchise with a squeaky clean image, is the target of a federal investigation into the hacking of the Houston Astros' player database sent shock waves through the sports world and beyond, but with several details yet to emerge, key questions remain.

The Cardinals' owner has said the breach is the result of the "roguish behavior" by a small group of individuals. Just days before the July Fourth holiday, the Cardinals fired head of scouting Chris Correa for what appears to be his connection to the hacking scandal. Still, the exact role Correa played, if any, in the alleged hacking is not known.

"We are in a situation where the public is really in the dark, and I think there is a lot more that can and will come out of this," attorney Jason B. Bonk, a litigator with Cozen O'Connor who handles complex commercial cases in several industries including sports, told Law360.

What Was The Extent Of The Breach?

The alleged breach revolves around Astros general manager Jeff Luhnow, who left the Cardinals front office to join the Astros in 2012. Luhnow is known for his use of analytics in evaluating players. It has been widely reported that he helped build the Cardinals' player database called Redbird, a concept he took with him to the Astros developing a similar system called Ground Control.

Both teams, which were division rivals before the Astros moved to the American League in 2013, are having strong seasons, with Astros' recent turnaround leaving them just one game off the lead of the American League West as July 19. Meanwhile, the Cardinals, a franchise with 11 World Series titles, most recently in 2011, are

perched atop National League Central.

According to the New York Times, investigators believe that the information accessed included discussions about player trades, proprietary statistics and scouting reports. It also reported the breach could have been as simple as former colleagues of Astros' front office personnel who left the Cardinals using old passwords. Also according to The Times, the FBI has traced a source of the breach to a computer in Jupiter, Florida, near the Cardinals training facility.

The FBI has not officially confirmed or denied the investigation, instead issuing a statement: "The FBI aggressively investigates all potential threats to public and private sector systems. Once our investigations are complete, we pursue all appropriate avenues to hold accountable those who pose a threat in cyberspace."

At this point, if anything else of value was obtained or whether there were more individuals or third parties involved is not publicly known. Although, The Houston Chronicle reported that the federal investigation is targeting up to four to five individuals within the Cardinals organization.

Furthermore, a statement issued by Correa's lawyer, Nicholas Williams, denying any wrongdoing, raises other suspicions as to the extent of the activity surrounding the alleged breach.

"The relevant inquiry should be what information did former St. Louis Cardinals employees steal from the St. Louis Cardinals organization prior to joining the Houston Astros, and who in the Houston Astros organization authorized, consented to, or benefited from that roguish behavior," the statement said.

Could Someone End Up In Jail?

FBI doesn't take such cyberthreats lightly, and the charges for the potential hack carry the possibility of serious prison time.

> "There is no question that these could be serious charges and there is no question that these charges can call for imprisonment," Eric Ostroff, a partner at Meland Budwick, P. A., focusing on business litigation and trade secrets law, said.

Multiple attorneys have pointed to potential criminal violations of two federal laws: the Computer Fraud and Abuse Act for the actual hacking and the Economic Espionage Act for potential theft of trade secrets.

The federal Economic Espionage Act takes its definition of trade secrets from the civil Uniform Trade Secrets Act, which has been adopted by most states, defining trade secrets as "all forms and types of financial, business, scientific, technical, economic or engineering information" that the owner has taken "reasonable measures" to keep secret and that "derives independent economic value, actual or potential, from not being generally known to … the public."

Under the act, violations could bring a fine of up to $5 million for organizations and are a felony for individuals, with a penalty of up to 10 years in prison.

The Computer Fraud and Abuse Act, which outlaws the accessing of a computer used in interstate commerce without authorization to obtain something of value, also has punishments for first-time offenders of a fine and/or one or five years in prison depending on the circumstances, and up to a possible 10 years, unless knowingly or recklessly causes serious bodily injury or death.

Will There Be Civil Suits?

Potential civil remedies for Astros are more complicated, and some attorneys say it here that the situation is unlikely to play itself out in the civil courts given the Cardinals' and Astros' relationship as members of MLB.

While the Computer Fraud and Abuse Act does provide a civil remedy, the federal Economic Espionage Act does not, meaning such claims would have to be brought under state law. There have been proposals in Congress to add a civil remedy, which could change the landscape of trade secrets litigation, but they haven't been adopted.

Further complicating matters is MLB's constitution, which prohibits teams from filing civil suits against one another and instead mandates that disputes be handled by the league with the commissioner as the arbitrator. However, this does not necessarily preclude a civil suit against individuals who may be guilty of wrongdoing or against third parties.

Ostroff noted that this is not a typical case of corporate espionage between two arm's-length competing companies. While the Cardinals and Astros compete on the field, they are essentially business partners as they are both entities in MLB. In a sense, what is best for baseball overall is best for both franchises.

"I think it would be highly unlikely that there would be an effort by the Astros to sue or seek relief directly from the Cardinals, but I suspect at the end of the day the Major League Baseball Commissioner Rob Manfred is going to have to issue some sort of sanction against those who are involved or against the team itself," Ostroff said. "That is likely where this would end because that makes is a unique corporate-espionage-type case. I'd be shocked if this played out in a courtroom."

How Have The Cardinals Reacted?

The Cardinals seem to already be taking proactive steps to protect the team's reputation and business interests. The organization have hired the St. Louis law firm of Dowd Bennett LLPto conduct an internal investigation.

And then there was the firing of Correa. Whether he was involved or not, the timing of the firing is interesting as it comes just after the MLB Draft and as the team is trying to sign its picks.

Lisa Sotto, a partner at Hunton & Williams LLP who specializes in privacy and cybersecurity issues, told Law360 that regulators look to see how an organization reacts to cyberattacks and whether actions are taken against those believed to be involved.

"To the extent that there was any wrongdoing, somebody typically bears the brunt of the discovery of that wrongdoing," Sotto said. "The first question a regulator will ask when examining a cybersecurity event is whether the employee that committed the untoward act has been disciplined. The Cardinals answered that question by firing this employee."

What's The Broader Impact?

While this may be the first situation like this in sports, this type of alleged behavior is not new to the corporate world. Having it occur in such a high-profile case should not only put other teams on notice, but other organizations and businesses outside

of sports as well.

Bonk pointed to reports that Astros' cross-state rival, the Texas Rangers, are undertaking an internal review of its network security in light of the hacking allegations and said other teams will follow their lead if they have not done so already.

"The broader issue is that the flag has been raised that compliance and risk management in this area is critical," Bonk said. "Until we know more, I think that it is incumbent on these teams and every team, and other companies in high profile areas to do what the Texas Rangers are doing."

And while this is a warning sign for other teams, regardless of whether this case ends in criminal charges, civil litigation or just MLB sanctions, attorneys say it is just a high-profile example of the types of dangers all companies face and emphasizes the importance of having good cybersecurity measures.

"I think every organization is subject to these sorts of cyberintrusions so nobody can afford to be complacent with respect to their cybersecurity framework," Sotto said. "Every organization, whether big or small, needs to consider the safeguards that they have in place to protect their business confidential information and they need to take proactive measures"