Hacking scandals highlight vulnerabilities for teams and leagues

CHRISTOPHER LAVIGNE

JEEWON KIM SERRATO

On April 3, the International Association of Athletics Federations announced that it had been the victim of a cyberattack, seemingly at the hands of Fancy Bear, a Russian hacking group. The IAAF indicated that the hackers targeted athletes' therapeutic use exemption applications which, if granted, allow athletes to use otherwise prohibited substances for therapeutic purposes (e.g. to treat illnesses). While this certainly is not the first instance of a hacking scandal in the world of professional sports, it and other recent incidents highlight the need for increased cybersecurity vigilance at sports organizations.

GETTY IMAGES

Teams and leagues have become attractive targets for hackers looking to disrupt or profit.

Recent cybersecurity scandals

Several hacking incidents over the past few years, involving the publication of confidential information or the defacement of websites, have been politically motivated. In addition to its recent hacking of the IAAF, Fancy Bear previously had hacked the World Anti-Doping Agency and published lists of Olympic athletes who filed TUE applications. According to Fancy Bear's website, its motivation was in "exposing the athletes who violate the principles of fair play by taking doping substances."

In a similar incident in 2015, Team Sky alleged that someone hacked into Tour de France champion Chris Froome's performance data as part of a campaign to prove that he is using performance-enhancing drugs.

In separate instances in 2014, an English rugby team's website was hacked by ISIS and FC Barcelona's Twitter account was hacked by the Syrian Electronic Army. In both cases, the hackers used the team's online platform to display their organizations' extremist messages.

While each of the preceding hacking incidents was seemingly perpetrated by hacktivists, another high-profile scandal demonstrates that hacking can be done for competitive purposes. Chris Correa, the St. Louis Cardinals' former director of baseball development, obtained a password from a former Cardinals employee who began working for the Houston Astros. Correa used the password to access an Astros email account and "Ground Control," a database used by the Astros to compile information on players such as scouting reports, statistics, contract information and draft rankings. Correa accessed Ground Control during the 2013 draft to view the Astros' internal, non-public information regarding undrafted players. Correa again accessed Ground Control before the 2013 trade deadline to view the Astros' internal, non-public information regarding its trade discussions with other teams. Correa pleaded guilty to criminal hacking charges and a federal judge principally sentenced him to 46 months imprisonment and ordered that he pay the Astros $279,038 in restitution.

Time can be [the] worst enemy in a cybersecurity breach.

Teams are vulnerable to attack not only through hacking, but also through social engineering. In 2016, the Milwaukee Bucks were victims of a phishing scam and released tax information, including Social Security numbers, of all its employees and players. An unknown party, impersonating Bucks President Peter Feigin, requested the information from a Bucks employee using a spoof email address.

Managing cybersecurity risks

With hacking incidents on the rise, teams are becoming attractive targets as they generate a significant volume of internal communications and confidential data. Through increased use of wearable technology and data analytics, professional sports teams can collect massive amounts of data on recruiting, training and performance evaluations, all of which are valuable targets to a whole host of actors, including competitors, gamblers and online "brokers" looking to sell this information to the highest bidder.

Teams and leagues also have incredibly sensitive information relating to the organizations' business dealings, including salary negotiations, sponsorships and advertising. And, of course, they retain and store payment card data from online transactions, all of which are classic targets for malicious cyberactivity. In short, professional sports teams and leagues can be an enticing prey for cybercriminal actors. The combination of valuable data, weak internal controls and poorly protected websites and social media accounts can be toxic in any industry.

So what to do about it?

One preventative measure that can be taken is to design a data governance system before any breach arises. Such a system would require implementing privacy policies and notices. In order to ensure the efficacy of a data governance system, a team should provide training on information security best practices to ensure that all employees take the appropriate security precautions in handling their computers and in safeguarding access to the team's systems. Since not all rogue behaviors or malicious actors can be prevented or stopped, having an incident response plan will best help organizations "game plan" various scenarios that could result in monetary or reputational damage.

The best offense is a strong defense, and effective incident response plans are critical in helping the organization calmly navigate its reaction to a cybersecurity breach. When properly tailored and thought through, such plans limit damage and dramatically reduce recovery time and costs. Indeed, time can be an organization's worst enemy in a cybersecurity breach, and incident response plans train the organization and its employees to respond quickly and efficiently, which has the net effect of limiting damage and managing employee concerns.

As we have seen, cybersecurity risks are no longer hypothetical in the sports industry as teams and leagues have become attractive targets. Promoting cybersecurity awareness and preparing an incident response plan are effective ways for members of this industry to protect their products and mitigate against any unauthorized intrusions. ■

Christopher LaVigne and Jeewon Kim Serrato are with New York-based Shearman & Sterling, a multinational law firm. Alan Goudiss and Chad Remus, also with Shearman, contributed to this column.