Dilworth Paxson

E-ALERT

Related Lawyers

Linda Dale Hoffa

Related Practices

White Collar/Government Investigations

Media Contact

Peter Dunn
Director of Client Relations and Communications
Philadelphia, PA
pdunn@dilworthlaw.com

WHAT IN-HOUSE COUNSEL CAN LEARN FROM MAJOR LEAGUE BASEBALL'S COMPUTER HACKING SCANDAL

July 28, 2015

LESSONS FROM MAJOR LEAGUE BASEBALL'S COMPUTER HACKING SCANDAL

Recent media reports revealed that the U.S. Department of Justice is investigating whether front office officials of the St. Louis Cardinals illegally hacked into the Houston Astros' networks to find information about the Astros' trades, proprietary statistics, and scouting reports. Front office employees of the Cardinals allegedly engaged in the hack to gain an unfair competitive advantage, as well as to get revenge against Astros General Manager Jeff Luhnow, who headed the Cardinals scouting and player development department before joining the Astros in 2011. The Astros only learned about the breach after some of their formerly secure data was posted to the website www.deadspin.com.

Some news reports claim that this security breach has the potential to be among Major League Baseball's worst scandals. But what is most striking about this scandal is that the alleged hacking was done so easily. According to law enforcement sources, the hacking into the Astros' on-line database was accomplished by St. Louis employees who simply located and then used passwords Luhnow had used when he worked for their baseball team. Could the hacking get any simpler than that? In fact, it's so simple, it hardly feels like a crime. But it is – and prior federal prosecutions demonstrate this.

In a case that garnered national press attention in 2008, federal prosecutors in Philadelphia charged and convicted Larry Mendte, a former TV news anchor, for computer hacking. For two years, Mendte was able to gain unlawful access to the private email accounts of fellow anchor Alycia Lane because he knew the passwords she used when the two had been friends.

Mendte pled guilty and admitted to distributing hundreds of Lane's private emails to newspaper reporters, gossip columnists, and others. He did this, according to the government's sentencing memorandum, "to spy upon, humiliate, and destroy the career of a co-worker – a person that he saw as a threat to his financial success." While Mendte was not sentenced to jail, he lost his job and, some would argue, his journalism career has never fully recovered.

More recently, in 2014, the CEO of a higher education software company committed a similar data breach involving two of his company's competitors. Ariel Manuel Friedler, former CEO and founder of Symplicity, admitted in federal court in Virginia that he and other Symplicity employees used their customer login credentials to gain access to competitor networks also used by their customers. After gaining access, Friedler and others in his company viewed proprietary and confidential

software design and features of competitors. The government alleged it was done to inform Symplicity's software development and sales strategies. For his crimes, Friedler was sentenced to two months in jail and lost control of his company.

The TV Anchor and the Software CEO wanted to know what their competitors were doing, and it was all too easy to do this by guessing passwords previously used.

The prosecutions of the TV news anchor, the software company CEO, and the investigation of the Astros' data breach, all involve the same federal criminal statute - a federal law called the Computer Fraud and Abuse Act (Title 18, United States Code, Section 1030). This statute imposes up to a five-year prison sentence if the intentional hacking has been committed without authorization and for the purpose of commercial advantage or private gain, or in furtherance of a tortious act. This federal law protects computers "used in or affecting interstate or foreign commerce or communications." Basically, that covers all computers connected to the Internet.

Most people think cyber crimes involve only intrusions committed by knowledgeable cyber criminals operating in foreign countries who steal large amounts of data for resale or hold systems hostage for ransom by using new and evolving methods to gain entries into protected computer systems. Few of these cases are successfully prosecuted given jurisdictional limitations and the need for international cooperation.

But the intrusions reportedly involved in the Astros' data breach, and in the Mendte and Friedler cases, involve unsophisticated actions that are easy for federal investigators to quickly prove and for federal prosecutors to charge. Businesses faced with similar opportunities to gain access to a competitor's computer system by using passwords from prior employees or from customers who now do business with the competitors can be tempting, but the lesson to be learned is this – don't do it. Guessing a password or having prior access to a password in order to gain entry to another's computer system without their knowledge or permission – even if done just to peek in and take a quick look – does not alter the fact that such conduct is a crime. Just because it is easily done does not provide one with a defense. Instead, it provides only a greater likelihood of being caught. And if caught, the consequences can include up to five years imprisonment and costly collateral consequences.