THE ARIZONA REPUBLIC
azcentral.com

Cybersecurity plan should address insider threats

Mark Pribish, Special to the Republic *7:22 p.m. MST January 14, 2016*

(Photo: Getty Images/iStockphoto)

STORY HIGHLIGHTS

- Employees are a significant cybersecurity threat.
- Small businesses are not immune to the threat of insider hacking jobs.
- Monitoring employees should be part of a prevention plan.

Employees do it for money or to pay back a perceived wrong. Some workers commit this form of sabotage because they didn't get a raise or promotion, or to help a friend.

Reports consistently show that employee hacking and cyberbreaches — known as the “insider threat," are your biggest threat when it comes to data breaaches and ID theft.

It’s three strikes and you’re out for a one-time MLB team employee. The Federal courts have focused on the activities of the St. Louis Cardinals baseball team as former Cardinals scouting boss Chris Correa has pleaded guilty to hacking the Houston Astros’ computer system.

According to the New York Daily News, “former St. Louis Cardinals scouting director Chris Correa pleaded guilty in Houston federal court to five counts of unauthorized access to the Astros’ player data base, in a case that gave new meaning to baseball sign stealing.”

This illegal breach happened because Correa was able to gain access into the Houston Astros’ computer network by obtaining the password of an Astro’s employee who had previously worked for the Cardinals. When the former Cardinal’s employee left the St. Louis Cardinals, the employee had to turn over his Cardinals-owned laptop and password to Correa.

Do you want to guess what happened next? Correa was able to use the old password of his former employee to guess the new password of his competitor.

Does this sound like corporate espionage of an international, Fortune 500 company? Absolutely. Can it happen to any size organization including your small business? Absolutely.

The fact is that any business is at risk of acts of sabotage from current and former disgruntled employees and several recent headlines are examples of the problems facing employers.But it gets worse. In the old days, disgruntled employees would “seek revenge” by stealing office supplies and bad-mouthing the boss.

Today, current and former employees are more likely to hack into your computer system to view and steal salary records, medical records, bank account information (e.g. for direct deposit purposes), driver’s license information, credit card information, and Social Security Numbers.

Additional “at risk information” being targeted by the insider threat includes proprietary company information and trade secrets, vendor information (e.g. server credentials like what happened to Target), and even cyber terrorists sabotaging data and networks such as the Sony hacking event from a terrorist state like North Korea.

And just when you think things can't get any worse than the above, you find out about an unhappy employee working as part of a conspiracy with outside hackers to attack your company.

“Some of the most costly data breaches originate from malicious insiders,” said John Iannarelli, a recognized expert on cybercrime and a former FBI special agent who now operates JGI Consulting Group.

Current and former employees intent on doing bad things typically have access to internal resources that outside hackers generally don’t have access to, said Iannarelli.

Companies — especially small to medium business — have to balance giving employees access to information while monitoring for suspicious or abnormal behavior, said Iannarelli. This can be done with a written, annually reviewed information security and governance plan signed by each employee to establish policies to safeguard proprietary and sensitive information from both cyber and physical loss, recommended Iannarelli.

Mark’s most important: Minimize your risk of a malicious insider by implementing a strong information security and governance plan which includes monitoring employees.

Mark Pribish is vice president and ID-theft practice leader at Merchants Information Solutions Inc., an ID theft-background screening company based in Phoenix. Contact him at markpribish@merchantsinfo.com.