THE ARIZONA REPUBLIC
azcentral.com

Businesses need to focus on the cyberenemy within

http://www.azcentral.com/story/money/business/tech/2015/07/09/small-businesses-cyberthreats/29947781/

Mark Pribish, Special for The Republic | azcentral.com | July 9, 2015

John Iannarelli, FBI cyberconsultant and recently retired assistant special agent in charge of the Phoenix division. (Photo: FBI)

"Small businesses are in denial about how vulnerable they can be to employees and vendors stealing proprietary company secrets and sensitive customer information," said John Iannarelli, FBI cyberconsultant and recently retired assistant special agent in charge, Phoenix division.

Recent stories have reported on how members of the St. Louis Cardinals baseball organization are under FBI investigation for hacking into a Houston Astros database

"This is corporate espionage and while uncommon in the sports world – it is very common in the business world," Iannarelli said.

Small- to medium-sized businesses need to protect their sensitive information such as customer or vendor lists, patented technology and processes, software code, unique business practices or intellectual property.

Iannarelli said that businesses need to consider two primary risks in protecting company information, including internal and external threats.

Internal threats can include current and former employees, vendors and customers who by malicious intent want to steal proprietary company and/or customer information for financial or intellectual gain – similar to the St. Louis Cardinals case.

Iannarelli said the more likely scenario is "accidental release," in which employees and vendors are not following information security and governance best practices" and accidentally lose confidential information.

The external threats can range from outside hackers to competitors. But a more likely example, according to Iannarelli, "is when a current employee accepts a position with a competitor and downloads company data prior to or after leaving the company."

For most small- to medium-sized businesses, information security and governance best practices, policies and systems are inadequate to prevent both internal and external threats – especially with employees stealing proprietary information.

So what can businesses do to protect themselves?

Iannarelli said that most can significantly minimize its risk with employees and/or competitors stealing company information by creating and implementing a formal information security and governance policy and plan that includes the following five points:

- Proprietary/confidential information. Define what proprietary/confidential information is and confirm which employees need access to it.

- Background screening. Determine if every employee or only those employees with access to proprietary/confidential information need to be background-screened.

- Employee information security education/training. Train employees on best practices, including Internet safety and how your business defines proprietary/sensitive information.

- Strong password management. Use 10-character passwords including lower- and uppercase letters, numbers and signs. Change passwords every 90 days.

- Software updates and patches. Most hacking events leverage old flaws that have already been addressed but that users simply haven't incorporated.

Using the Cardinals-Astros case as an example, Iannarelli said that every small business should consider:

- How will the reputation of the Astros be impacted knowing their database was so vulnerable?

- How much of the Cardinal's reputation will be tarnished based on an employee (and possibly other employees) knowledge of hacking, unethical and unlawful behavior?

- Did both organizations have a formal information governance policy in place defining best practices and prohibiting such actions?

Mark's most important: Business owners who want to remain in business must take cybersecurity seriously and recognize that one of the biggest threats is within the organization.

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