Does Being Fit Increase Your Company's Risk of Security Breaches?

Insights
2.14.18

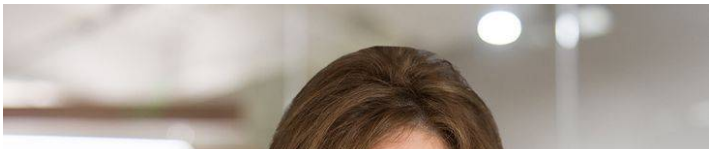
As we are early into the new year, for many, hope springs eternal to get in shape during 2018. Many of us wear some kind of fitness activity tracker that monitors steps, heart rate, calories, sleep patterns, etc. Recent news coverage of Strava, the running and cycling fitness tracking app, has caused concern for the United States military. But might it cause concerns for some businesses that operate under high levels of security, as well?

In November 2017, Strava released a heat map demonstrating activity tracked by its app users, placing these routes on a real-world map. The map compiled more than 3 trillion individual GPS data points depicting every activity ever uploaded to Strava from personal fitness tracking devices. In late January 2018, it was reported that the U.S. military found that the map also provided enough information to identify secret military bases, due to active military personnel using the app.

Although the companies that host these fitness tracking devices have privacy policies that promise to keep personal data secret, many also reserve the right to use data shared by its users in aggregated and anonymous forms. The aggregated data published by Strava's heat map is seemingly enough to identify top-secret military facilities, along with the travel paths of its personnel. The same can be said for employees of companies that operate under high levels of secrecy and security, or any company for that matter.

Most businesses have not considered the security implications associated with its employees wearing these activity trackers while working, and what information is being relayed through these devices to the host company, as well as through any other apps to which the employee may choose to subscribe. This most recent discovery via the Strava map may cause some businesses to reexamine whether employees should be wearing these trackers while working, or whether there are other privacy and security settings that the user can control through the device or app to limit the information shared.

Related People



Michelle I. Anderson
Partner
504.529.3839
Email