Is Your Company Car Exposing Sensitive Data To Hackers?

Insights
1.01.18

If your business is like most others, you probably store a lot of sensitive data in an electronic format. And if your business takes proper precautions, you probably utilize sophisticated cybersecurity systems to prevent the hacking of such data. You likely also require your employees to password-protect their phones, and perhaps even download security software applications for added protection. But have you considered potential data vulnerabilities posed by your company cars and your employees' cars? Likely not, but there is convincing evidence that you should start.

Auto Infotainment Systems: The Next Hacking Frontier

According to a recent article published by the webzine Motherboard, cars are a potential treasure trove of unsecured data just waiting for a hacker to claim it. A security software engineer discovered that his car's infotainment system did not use modern security software principles, yet it stored an unbelievable amount of personal data obtained from his phone – including contact information, texts, emails, call histories, as well as directory listings that had been synchronized with his car via Bluetooth and other similar connections. Worse, he discovered this information was being stored on the car's infotainment system in plain, unencrypted text.

He surmised that unscrupulous hackers could gain access to this information remotely through his in-car internet connection, a quickly growing technology, or directly through the car's USB port. Although mobile operating systems like Google Android and Apple iOS use highly effective security protections, these protections could be undone simply by pairing mobile devices to the car's infotainment system.

We don't know to what extent the issue exists among the various car models manufactured each year, but this revelation should raise several concerns for your business. If employees sync their mobile devices to a company car's infotainment systems, they could be unintentionally storing personal data on the car's system, making it susceptible to hackers. Similarly, if an employee uses a company-issued or personal mobile device for work that is paired to a company car, or even a personal vehicle, sensitive company information such as customer lists and contact info may be stored in the car and, therefore, vulnerable.

What Should You Do?

How should you deal with this apparent security risk? Unfortunately, there are no easy fixes at present. Car manufacturers are just now beginning to discuss how to address data security issues created by their cars. For companies with a fleet of cars, however, you should contact the car

manufacturers to inquire about the security of the firmware (the embedded software) used in the cars. You should remain in contact with the car manufacturers to make certain you will be notified if there are tech-related updates or recalls. If the manufacturer indicates the car's firmware needs updating, ensure this is done as soon as possible, even it means taking the car to the dealership.

If employees are responsible for company car maintenance, or if they use their personal cars for work, you should have a policy requiring employees to update the car's firmware within a set period of time following the release of the update. You may also want to consider prohibiting employees from syncing their mobile devices to company vehicles or syncing company-issued mobile devices to their personal vehicles.

In this age of car connectivity, auto manufacturers are working on developing more secure systems to protect the data collected by cars. Until those systems are a reality, however, you need to be aware of the potential data security risks posed by some cars and take whatever steps you can to help reduce that risk.

For more information, contact the author at MGomsak@fisherphillips.com or 502.561.3972. This article originally appeared on the firm's Employment Privacy Blog.

Service Focus

Privacy and Cyber