Is Your Vehicle One of the Most Hackable Cars?

Here's a top five list you probably don't want your car to be in: the most hackable cars on the road.

PT&C LWG Forensic Consulting Services compiled a list of cars with the highest risk of being hacked. The top five and the reasons are:

- 2014 Jeep Cherokee, which it said is the only vehicle to be recalled due to potential hackability.
- 2014 Infiniti Q50, which was recalled because its Direct Adaptive Steering software could potentially disable the power steering software when the engine compartment reached freezing temperatures.
- 2015 Cadillac Escalade, which is hackable because the car's apps, Bluetooth, and telematics are on the same network as the engine controls, steering, brakes, and tire pressure monitor system.
- 2014/2010 Toyota Prius, which was recalled due to faulty software in the car's hybrid-control system.
- 2014 Ford Fusion, which allows hackers to control some of the car's features from anywhere.

"In general, a hacker can be anywhere from five to 100 meters away from the targeted car, depending on the hacking method; however, if hacking over Wi-Fi, the hacker could be anywhere with Internet access," the report found. "The hack typically occurs in three stages. First, the hacker compromises one of the computer systems remotely. Next, the hacker sends messages to cyber-physical components, and then finally makes the destination engine control unit perform some desired action. Parts of your car that might be affected can include the ignition system, the brakes, door locks, and other systems of your car."

The company said that automobile manufacturers "have been slow to publicly admit to the dangers of their cars being hacked." However, recent high profile car hacks "have refocused their efforts to be more transparent on the development of security features that protect their vehicles from hackers."

They found the least hackable cars are: 2014 Audi A8, 2014 Dodge Viper, 2014 Honda Accord, and Tesla Model S.

What remains unresolved are the legal issues as to who is liable for accidents, injuries, and damages resulting from the hacking, issues explored earlier and in a panel discussion chaired by Richard Balough at this week's American Bar Association Business Law Section Annual Meeting in Chicago. Balough Law Offices also explored these issues in an earlier article in Business Law Today available at http://www.balough.com/balough-cyberterrorism-on-wheels-article-published-by-aba.

Balough Law Offices, LLC, is a Chicago-based law firm which focuses on cyberspace, business, and intellectual property law. Our homepage is balough.com.