Published on *The National Law Review* https://natlawreview.com

# Cybersecurity: Yes, They Will Hack Your Car

Article By:

Christopher H. Grigorian

R. Nicholas Englund

Auto manufacturers are increasingly equipping vehicles with rapidly advancing technologies, raising concerns regarding how the public will be affected by these changes. Manufacturers are beginning to implement automated driving and vehicle-to-vehicle (V2V) communication capabilities into their cars, extending potential cybersecurity threats and associated safety issues to road users.

As consumers, we already see cybersecurity threats and breaches in many areas of our day-to-day lives. With the spike of auto-driven and connected cars across the auto industry, these same threats and breaches have a strong potential to sprout in our lives on the road as well.

NHTSA has outlined the factors it will consider in evaluating cybersecurity threats as potential safety-related defects. They are as follows:

- The amount of time elapsed since the vulnerability was discovered (e.g., less than one day, three months, or more than six months)
- The level of expertise needed to exploit the vulnerability (e.g., whether a layman can exploit the vulnerability or whether it takes an expert to do so)
- The accessibility of knowledge of the underlying system (e.g., whether how the system works is public knowledge or whether it is sensitive and restricted)
- The necessary window of opportunity to exploit the vulnerability (e.g., an unlimited window or a very narrow window)
- The level of equipment needed to exploit the vulnerability (e.g., standard or highly specialized)

Additionally, NHTSA’s guidance suggests policies that manufacturers :

- Participating in the Automotive Information Sharing and Analysis Center (Auto-ISAC), which became fully operational in January 2016

- Developing policies around reporting and disclosure of vulnerabilities to external cybersecurity researchers
- Instituting a documented process for responding to incidents, vulnerabilities, and exploits and running exercises to test the effectiveness of these processes
- Developing a documentation process that will allow self-auditing, which may include risk assessments, penetration test results, and organizational decisions
- For original equipment, developing processes to ensure vulnerabilities and incidents are shared with appropriate entities throughout the supply chain
- As vehicle technologies continue to progress, we expect that NHTSA’s guidance will evolve to address future concerns

To continue reading through NHTSA’s enforcement plans on motor vehicle safety as it pertains to recent technological advances, be sure to check out Thursday’s post on automated vehicle regulations.



National Law Review, Volume VII, Number 68