CYBER
INSIGHTS

LloydSadd

NAVACORD®

Your Vehicle May Be at Risk for a Cyberattack

You've seen the reports: Hackers remotely take over a moving vehicle or exploit a key fob to enter and steal an electric car. Many high-profile auto hacks have proven that cybersecurity vulnerabilities exist within the industry.

Modern cars operate on computer networks. Even the most basic gas-powered models use dozens of semiconductor chips. Emerging cellular networks are increasing as rapid technological advances struggle to maintain strong cybersecurity protocols.

Cybercriminals are capitalizing on this connectivity, exploiting weak links.

TECH CAN INCREASE YOUR CAR'S RISK OF A CYBERATTACK

Like a computer network, your car's connected devices may have weak points that cybercriminals can exploit, such as:

- Mechanisms that use smartphone-driven digital keys or near-field communication cards to unlock and start your vehicle. Criminals can hijack the wireless signals to steal your car later.
- Connectivity. Connectivity creates a seamless consumer and entertainment experience. It also creates cybersecurity flaws in your vehicle due to cellular networks, Wi-Fi, device dongles and physical connections. Criminals can swipe your personal information, including addresses, financial and banking information, trip planners, GPS data, and onboard entertainment information and preferences.
- In-vehicle infotainment that combines apps like social media and banking for seamless experiences. Examples include fuel payments, toll payments, parking and trip planning.
- Advanced driver assistance systems. These use an interconnected series of sensors, cameras and semiconductor chips to operate. Park assist, blind spot detection and tire pressure monitoring are examples.
- Autonomous driving systems. Rapidly emerging tech like light detection and ranging (or "lidar") uses laser pulses to create 3D mappings of the car's environment. It can detect objects like buildings, roads, vehicles and pedestrians. Lidar technology helps the vehicle sense and understand its surroundings. But criminals can spoof lidar using adversarial lasers to blind vehicles, which could cause accidents or damage.

WHO'S AT FAULT: DRIVERS OR CYBERCRIMINALS?

From an insurance perspective, the answer is unclear.

Insurance companies may eventually include coverage for onboard connectivity, as part of a stand-alone cyber liability policy or an add-on to your auto coverage. But right now, most auto policies remain silent about damage due to cyberattacks.

Staying silent on an issue is sometimes preferable to outwardly excluding something. If there is no mention, you can try to appeal the decision if the claim is denied.

Until policy language changes, most data breaches will fall under the cyber or data breach insurance category.

CYBER LIABILITY OR DATA BREACH INSURANCE

As for personal data breaches from attacks on cars, a personal cyber policy might cover you. Check the exclusions. These can vary significantly by company.

Ask your insurance broker to clarify loss scenarios involving cyberattacks like:

- A hack resulting in loss of control of the vehicle, causing bodily injury or physical damage
- A hack resulting in data theft only
- A hack that damages the car's onboard computer system but causes no physical damage to others

AUTO MANUFACTURERS OFFERING INSURANCE

Some auto manufacturers offer vehicle-specific insurance designed to handle the parts and peripherals. However, these policies may be like traditional auto policies that address bodily injury or property damage, but not data breaches. Don't assume you're covered for cyber insurance just because the manufacturer is offering the policy. Check the language.

USE YOUR CYBERSECURITY KNOWLEDGE

Think of modern vehicles as networks that interact with external devices as they move through the world. Handle vehicle cybersecurity like you'd handle your device or home network security. Stay informed and maintain your cybersecurity senses when using your vehicle:

- Use a PIN to start your vehicle as an added layer of safety.
- Use encryptions for all sensitive data, including access to your vehicle's digital keys.
- Ask manufacturers and vendors about default admin accounts (or system backdoors) that could compromise your data security.
- Install updates to your vehicle's onboard and connected systems as soon as they're available.
- Use only secure internet connections to update your vehicle's systems.
- Charge your electric vehicle at manufacturer-recommended or reputable charging stations.

CALL YOUR INSURANCE BROKER

Your broker can help you navigate emerging auto liability exposures. Your insurance policy language determines your coverage, and your broker can help you find the proper coverage for your situation.

If you have questions specific to your business, or would like additional information, please reach out to your Lloyd Sadd Advisor.

™®Local Touch. National Strength. Navacord and Navacord logo are Trademarks of Navacord. The information contained herein is general in nature and general insurance description only. The information is not intended to be insurance advice; nor does it amend, modify or supplement any insurance policy. Consult your actual policy or your broker for details regarding terms, conditions, coverage, exclusions, products, services and programs which may be available to you.

LET US HELP YOU MANAGE YOUR RISK

Edmonton: 1.800.665.5243
Calgary: 1.866.845.8330
Kelowna: 1.800.665.5243

lloydsadd.com
info@lloydsadd.com

Local Touch. National Strength.™