RISK INSIGHTS

SCS AGENCY INSURANCE

General Cybersecurity Best Practices for Modern Vehicles

Modern vehicle technology has transformed in the past several years as autonomous driving, vehicle electrification and car connectivity features have become more common. While these digital innovations in the automotive industry have added significant customer value, they have also exposed vehicles to cybercriminals attempting to gain access to critical in-vehicle electronic units and data. This article discusses cybersecurity threats modern vehicles face, the importance of the automotive industry providing protections against those risks and best practices for minimizing cybersecurity threats.

Cybersecurity Threats in Modern Vehicles

These days, vehicles are becoming increasingly dependent on connectivity and technology that runs complex software. There are about 100 million lines of software code in today's vehicles, and by 2030, they're expected to have roughly 300 million. The overabundance of complex software code within vehicles offers ample opportunity for cyberattacks.

Cyberattacks on modern vehicles could endanger vehicle inhabitants and others, and they may also be used to track vehicles or related data. Hackers can accomplish these attacks through physical or remote avenues:

- **Physical access**—When hackers gain physical access to a vehicle's internal communication system, they can affect vehicle operations, such as steering, acceleration and braking.
- **Remote access**—Modern vehicles utilize Bluetooth technology, remote start applications and GPSs. Once hackers gain remote access, they can transfer knowledge from computers to vehicles and vice versa.

Importance of Cybersecurity in Modern Vehicles

While in-car cybersecurity threats are still relatively new, they are an ongoing concern. It is now the responsibility of automakers to consider cybersecurity an integral part of their core business functions and development efforts. Systems and components that govern vehicle safety features must be protected from harmful attacks, unauthorized access, damage or other threats that might interfere with safety functions.

Best Practices

A layered approach to vehicle cybersecurity can help reduce the probability of an attack's success and mitigate the ramifications of unauthorized system access. The following are general best practices for modern vehicle cybersecurity:

- **Leadership priority on product security**—An emphasis on mitigating cybersecurity challenges associated with motor vehicles and motor vehicle equipment should be a priority for automotive industry suppliers and manufacturers. By stressing the importance of cybersecurity from the leadership level down to the staff level, corporations can emphasize the seriousness of managing cybersecurity risks and

prioritize cybersecurity throughout the product development process.

- **Vehicle development process with explicit cybersecurity considerations**—The entire lifecycle of a vehicle—conception, design, manufacture, sale, use, maintenance, resale and decommission—should be taken into consideration when addressing cybersecurity risks, especially since there is more flexibility to design and implement protective measures early in the development process.

- **Information sharing**—In late 2014, the National Highway Traffic Safety Administration (NHTSA) encouraged the automotive industry to establish Auto-ISAC, an industry-driven community for sharing and analyzing intelligence about emerging cybersecurity risks to vehicles. Vehicle manufacturers, automotive equipment suppliers, software developers, communication services providers, aftermarket system suppliers and fleet managers are strongly encouraged to join Auto-ISAC and share timely information concerning cybersecurity issues.

- **Security vulnerability reporting program**—Members of the automotive industry should make information reporting easy for the security research community and the general public to help identify cybersecurity vulnerabilities.

- **Organizational incident response process**—While it's not possible to predict all future attacks, organizations can prepare their responses, processes and staff to handle incidents effectively. Organizations should develop a product cybersecurity response process that includes:

    - A documented incident response plan
    - Roles and responsibilities that are clearly identified within the organization
    - Communication channels and contacts outside of the organization that are clearly identified
    - Procedures for keeping information up to date

- **Self-auditing**—To establish a clear and controlled process for managing software and related vulnerability risks, organizations must ensure documentation and document controls are in place. For process management documentation, members of the automotive industry should:

    - Document the details related to their vehicle cybersecurity risk management process
    - Retain documents through the expected lifespan of the associated part
    - Implement and follow a control protocol

  To assist companies in better understanding their cybersecurity practices and how to improve them, procedures for internal management and documentation review should also be established.

- **Education**—Continuous education of existing and future workforces can assist in improving the cybersecurity of motor vehicles. NHTSA encourages vehicle manufacturers, suppliers, universities and other stakeholders to work together to support the educational efforts of the workforce.

- **Aftermarket/user-owned devices**—Aftermarket devices, such as insurance dongles, and user-owned devices, such as cellphones, could present unique cybersecurity challenges. Before these devices are connected to vehicle systems through interfaces provided by the manufacturer, they should be authenticated and provided with appropriate, limited access.

- **Serviceability**—The average motor vehicle requires regular maintenance and occasional repair to operate safely. The automotive industry should consider the serviceability of vehicle components and systems since vehicles can remain in use for over a decade.

Conclusion

The automotive industry can work towards protecting electronic systems, communication networks, control algorithms, software, users and underlying data from malicious attacks, damage, unauthorized access or manipulation by implementing cybersecurity best practices. Contact us today for more risk management guidance.