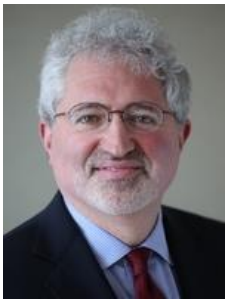
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Inside NHTSA's Proposed Cybersecurity Best Practices

By **attorneys at Crowell & Moring LLP**



Scott L. Winkelman

Peter B. Miller

Kate M. Growley

Law360, New York (November 15, 2016, 12:59 PM EST) -- On Oct. 24, the National Highway Traffic Safety Administration proposed a set of voluntary cybersecurity best practices for manufacturers and designers of vehicle systems and software. Consistent with its July 2015 discussion of vehicle cybersecurity, NHTSA's proposals focus on hardening system architecture to reduce the overall risk of attacks and designing safeguards to permit safe and appropriate vehicle action should attacks succeed. Utilizing a deliberately flexible approach to address "cybersecurity vulnerabilities [that] could impact safety of life," NHTSA calls for vehicle stakeholders to make cybersecurity "an organizational priority" and to develop a "risk-based approach" to confront dynamic cybersecurity threats.

Key Recommendations

By and large, NHTSA's proposed best practices build on pre-existing standards. Central is the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which has already been widely accepted by public and private sector entities, including the Federal Trade Commission. The framework employs an iterative and flexible approach to managing cybersecurity risk, centered on five core principles:

- Identify (developing the organizational knowledge, culture and commitment necessary to understand, manage and reduce risks associated with the organization's activities);
- Protect (developing appropriate controls to reduce risks);
- Detect (developing appropriate activities to detect cybersecurity events);
- Respond (developing ability to respond appropriately to cybersecurity events); and
- Recover (developing resiliency and ability to timely return to normal operations).

NHTSA recommends that industry also adopt other widely accepted cybersecurity standards and practices, such as the ISO 27000 series, the Center for Internet Security (CIS) Critical Security Controls, security-by-design principles, and information-sharing through the Auto ISAC (Information Sharing and Analysis Center).

Among NHTSA's more specific recommendations, it urges that vehicle stakeholders:

- Tightly control software developers' post-sale access to onboard technology;
- Protect cryptographic and password keys used to access or diagnose vehicle electronic systems by enabling them each to access a single vehicle, not multiple vehicles;
- Limit internal and external ability to access diagnostic tools, or access and modify firmware, including by restricting the functionality that can be affected;
- Minimize and safeguard communications to back-end servers, communications between vehicle systems, and the vehicle's connection to wireless networks, including through use of message authentication and encryption when appropriate;
- Isolate and segment processors, networks and external connectors, and minimize unnecessary network services;
- Maintain an "immutable log of events" to support threat assessment and to permit reconstruction of events and analysis of flaws if a breach occurs;
- Enact self-auditing programs that include periodic risk assessments, rigorous cybersecurity testing and regular self-review;
- Anticipate and address cybersecurity issues associated with aftermarket devices and components; and
- Protect serviceability and consumer choice by avoiding cybersecurity protections that "unduly restrict access by authorized alternative third-party repair services."

Legal Significance

The just-released NHTSA guidance is nonbinding. It does, however, suggest that NHTSA may eventually utilize its safety mandate "to cover vehicle cybersecurity." Recent enforcement actions in other contexts demonstrate that voluntary best practices can over time become enforceable — for example, by the FTC with regard to the NIST Cybersecurity Framework, or by the California attorney general with regard to the CIS Critical Security Controls. NHTSA's principles may foreshadow regulatory or legislative action to come.

Still, few of the cybersecurity principles announced by NHTSA's proposed guidance are novel. Many are contained within existing best practices documents like the Auto Alliance's Cybersecurity Best Practices and the Society of Automotive Engineers' Cybersecurity Guidebook. The guidance in these documents, like NHTSA's proposed guidance, requires auto manufacturers to (1) design vehicles for security, (2) assess and manage risk, (3) detect and protect against threats, (4) develop plans to respond to and recover from incidents, and (5) share threat and vulnerability information.

NHTSA's guidance in essence encourages the continued development and implementation of these self-governing standards.

Broader Context

NHTSA's guidance comes in the midst of the agency's drive to improve cybersecurity practices. Just weeks ago, the agency issued its Federal A.V. Policy, which contained extensive cybersecurity directives tailored to highly automated vehicles. NHTSA urged Congress in January 2016 to enact heightened safety standards for motor vehicles equipped with onboard electronic systems. And in the summer of 2015, the agency ordered the recall of more than 1.4 million vehicles after two researchers wirelessly hacked into a dashboard connectivity system.

The guidance is also consistent with broader federal, state, and private sector cybersecurity activities. An alphabet soup of federal agencies have announced cybersecurity initiatives, guidance, regulations and/or enforcement actions, including the Consumer Financial Protection Bureau, U.S. Commodity Futures Trading Commission, U.S. Department of Homeland Security, U.S. Department of Defense, U.S. Department of Education, U.S. Department of Energy, U.S. Department of Justice, Federal Communications Commission, Federal Trade Commission, U.S. Department of Health and Human Services, and U.S. Securities and Exchange Commission. The National Conference of State Legislatures identifies at least 26 states that have considered cybersecurity legislation this year alone. In addition, private plaintiffs are increasingly viewing failures in cybersecurity design, implementation and execution as an attractive litigation focus in recent hackability cases.

The guidelines themselves encompass established best practices and emerging trends. For example, the guidelines (unsurprisingly) encourage information sharing. Both regulators and industry embrace information sharing, which has been a consistent theme in recent cybersecurity initiatives. In June of this year, the U.S. Department of Homeland Security and the DOJ issued joint guidelines on voluntary sharing of cyber threat indicators. Then in September, HHS recommended that entities covered under the Health Insurance Portability and Accountability Act share threat information. HHS has even launched a monthly "Cyber Threat Sharing Newsletter" to that end.

More specifically to the auto industry, NHTSA encouraged in 2014 the creation of an Auto ISAC, where members could discuss threats, trends and best practices. This ISAC became fully operational in January of this year. And, although many industry members have joined the ISAC, NHTSA encourages "all members of the vehicle manufacturing industry" to join. The Auto Alliance also embraces information sharing as one of its five core principles. Specifically, it recommends "building partnerships across the vehicle ecosystem, including sharing of cyber threat trends and proven techniques with third parties to defend against cyberattacks."

Given how popular information sharing has become, members of the auto industry that do not join the Auto ISAC may find themselves missing out on information about emerging threats and consensus best practices, potentially falling short of developing industry cybersecurity norms. The end result may be that they cannot fully benefit from arguing their adoption of "reasonable cybersecurity measures, consistent with industry practices," should an enforcer or private litigant later challenge their cybersecurity-related activities.

Conclusion

This NHTSA guidance represents the agency's latest foray into establishing cybersecurity standards for the auto industry. It steers cybersecurity toward risk-management practices that are, for many, already best practices. The guidance also continues the trend toward harmonizing federal agency interpretations of reasonable cybersecurity practices around well-established public- and private-sector principles. While the guidance is nonbinding, it is both substantive and consequential. No one should be surprised if it foreshadows law to come.

To read this guidance in its entirety, visit this link. NHTSA will be accepting comments regarding its proposed cybersecurity best practices until Nov. 28, 2016.

Scott L. Winkelman is a partner and chairman of the product liability and torts group at Crowell & Moring LLP in Washington, D.C.

Peter B. Miller is a senior counsel in Crowell & Moring's advertising and product risk management and privacy and cybersecurity groups in Washington, D.C. He previously served as chief privacy officer at the Federal Trade Commission and safeguarded personal information throughout its life cycle at the agency.

Kate M. Growley, Danielle Rowan and Justin Kingsolver are associates at Crowell & Moring in Washington, D.C.