wiley

NEWSLETTER

Security Discussions – Are ISACs' Operations Vulnerable to Third Parties?

December 2017

In 2015, *WIRED* magazine brought public attention to a claimed cybersecurity vulnerability in the entertainment systems of certain vehicles.[1] This software vulnerability allegedly allowed security researchers to hack the vehicles and take control of various elements, from dashboard functions to steering.[2] Following this report, over a million vehicles were recalled,[3] and some owners and lessees of the vehicles initiated class action litigation – *Flynn v. FCA* – over the alleged flaw.[4] While research exposed alleged vulnerabilities in entertainment systems, the ongoing litigation has exposed vulnerabilities in the current approach to cybersecurity information sharing and the need for a policy solution.

ISAC Vulnerability

Specifically, in the summer of 2016, the plaintiffs in *Flynn* served a subpoena on the Automotive Information Sharing and Analysis Center (Auto-ISAC) seeking, among other things, communications between the defendant automaker and the non-party ISAC. The ISAC was able to successfully fend off the subpoena. The court ordered the subpoena to be quashed, agreeing with the Auto-ISAC that the subpoenaed documents were not relevant to the underlying case.[5] The subpoena, despite being quashed, reveals real weaknesses in the current U.S. approach to cybersecurity information sharing.

The importance of cybersecurity information sharing cannot be overstated. Industry needs to be able to share information about threats and countermeasures, among other things, with each other and with government to effectively combat the ever-evolving threat landscape. Robust legal protections are needed to ensure that companies can voluntarily engage actively in real-time sharing

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

without the threat of liability. Congress recognized this and passed the Cybersecurity Information Sharing Act of 2015 (CISA), which promotes and protects voluntary information sharing.[6]

ISACs are important venues for information sharing. The idea for sector-specific ISACs formed in the late 1990s,[7] and today, there are more than 20 sector-based ISACs serving as information-sharing hubs for critical infrastructure industries ranging from the automobile industry (Auto-ISAC) to the communications industry (COMM-ISAC). These organizations "collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency"; they also coordinate across sectors.[8]

However, despite federal policy to promote voluntary information sharing – from CISA and through the ISAC infrastructure – there remain risks associated with information sharing, as highlighted in *Flynn*. There is little to stop another set of plaintiffs in another class action lawsuit from seeking communications between companies and their ISAC, and another court may reach a different conclusion than the *Flynn* court did.

The Resulting Risk

The mere suggestion that communications with information-sharing organizations are not protectable may have a chilling effect on companies' willingness to share information. This outcome is unacceptable, given the critical importance of cybersecurity and information sharing. Policymakers should work with urgency to fully protect entities involved in cybersecurity information sharing, and ensure that all cyber communications remain protected.

[1] Hackers Remotely Kill a Jeep on the Highway (July 21, 2015), available here.

[2] After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix (July 24, 2015), available here.

[3] After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix (July 24, 2015), available here.

[4] *Flynn v. FCA U.S. LLC and Harman International Industries, Inc.*, Case No. 16-mc-00078 DGW (S.D. Cal.).

[5] *Flynn v. FCA and Harman International Industries, Inc.*, Order, Case No. 16-mc-00078 DGW, at 6 (S.D. Cal. Nov. 30, 2016).

[6] Pub. L. 114-113, 6 U.S.C. § 1501.

[7] *See* here.

[8] National Council of ISACs. *See* here.