Hi All,

Please find attached the Weekly Automotive Industry Report covering April 3 - April 8.

This week's report includes articles on:

- Toyota partnering with Microsoft on a new cloud-based division led by the CIO,
- Intel acquiring a semiconductor manufacturer that builds chips for self-driving cars,
- Hyundai unveiling its connected vehicle "roadmap," and,
- Toyota planning to open a new autonomous vehicle research center in Michigan.

You can find past reports on site.

Please let me know if you have any questions. Have a great weekend.

Josh

---

Auto-ISAC Executive Overview
SANS Presentation

02 May 2017
Introductions
Automotive risk landscape
Auto-ISAC overview
Membership highlights
Next steps
Transforming through connectivity

Consumers are asking for:
- Safety
- Entertainment
- Convenience
- Enhanced consumer experience

The commercial vehicle sector is seeking:
- Safety
- Efficiency
- Predictive maintenance
With connectivity comes cyber risk

<table>
<thead>
<tr>
<th>Vehicle Features</th>
<th>Yesterday</th>
<th>Today</th>
<th>Tomorrow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensors</td>
<td>Automated Assist</td>
<td>Apps</td>
<td>Cellular Modem</td>
</tr>
<tr>
<td>Gov’t Interest</td>
<td>IT Standards</td>
<td>Privacy Legislation</td>
<td>Markey Report</td>
</tr>
<tr>
<td>Attack Scenario</td>
<td>Single Vehicle Spoofing and Manipulation</td>
<td>Remote Control</td>
<td>Wide-Scale PII Theft</td>
</tr>
<tr>
<td>Threat Actors</td>
<td>White Hat: Academic Research</td>
<td>White Hat: Popular Media</td>
<td>Criminal, Hacktivist, Terrorist and Nation State</td>
</tr>
<tr>
<td>Attack Vector</td>
<td>Physical</td>
<td>Software and Apps</td>
<td>Supply Chain</td>
</tr>
<tr>
<td>Business Impact</td>
<td>Minor Disruption</td>
<td>Major Business Disruption</td>
<td></td>
</tr>
</tbody>
</table>

Risk is increasing and will continue to grow...

Automakers recognized the growing vehicle cyber risk, and, in 2015, proactively joined together to form the Auto-ISAC.
Why did OEMs join together?

Organizations must act individually to manage cyber risk...

...and one’s detection is another’s prevention.

- Identify emerging threats and vulnerabilities earlier
- Pool limited resources to better fight your adaptive adversary
- Share incident intelligence to act more quickly
- Proactively shape industry-wide best practices
- Protect overall trust in innovation across the industry
- Build resiliency across industry
Why an ISAC?

ISACs are the result of Presidential Decision Directive 63 (PDD-63)

In 1998, PDD-63 emphasized that 90% of the nation’s critical infrastructure* is owned and operated by the private sector.

It asked each industry to create a sector-specific organization to share information about physical and cyber threats, vulnerabilities, and incidents.

Today, there are 24 ISACs that serve this role.

Other policies enabling ISACs include:

|------------------------------------------|---------------------------------------------------------------|----------------------------------------------------------------------------------|
Introduction to Auto-ISAC

Key Achievements

- **Dec 2015:** Auto-ISAC formed
- **Feb 2016:** Expanded membership to suppliers
- **July 2016:** Exec Sum of auto cyber security best practices released
- **Nov 2016:** Expanded membership to heavy-duty vehicle OEMs & suppliers
- **Jan 2016:** Expanded membership to commercial vehicle sector
- **Jan 2016:** Auto-ISAC Portal launched
- **July 2016:** Auto-ISAC vehicle cyber incident response wargame
- **Oct 2016:** Onboarded Executive Director

Membership represents **99%** of cars on the road in North America

- **15** OEM Members
- **18** Supplier Members
- **6** Strategic Partners

- **>250** active users
- **360+** intel sources
- **25+** speaking engagements

Members from **7** countries on 3 continents

- **130+** intel reports
- **150+** media mentions
- **1** Best Practice Guide complete, 6 more planned

Coordination with **23** critical infrastructure ISACs through the National ISAC Council
Overview of Auto-ISAC operations

**Mission**
Serve as an unbiased information broker to provide a central point of coordination and communication for the global automotive industry through the analysis and sharing of trusted and timely cyber threat information.

**Scope**
Light- and heavy-duty vehicles, commercial vehicle fleets and carriers. Currently, we are focused on product cyber security, and anticipate expanding into manufacturing and IT cyber related to the vehicle.

**What We Do**

- **Intel Sharing**
  Data curation across intel feeds, submissions and research

- **Analysis**
  Validation, context and recommendations

- **Best Practices**
  Development, dissemination and maintenance

- **Partnerships**
  Industry, academia, vendors, researchers and government

**Community Development**
Workshops, exercises, all hands, summits and town halls
**Member benefits**

**Find and fix issues faster.**
Time is money, especially in cyber. Members receive verified, timely cyber threat, vulnerability, and remediation information.

**Maintain a trusted brand.**
Customers demand safety and privacy. OEMs demand secure components from suppliers. Joining the ISAC demonstrates a commitment to protecting vehicles, services and, ultimately, drivers.

**Stay ahead of regulation.**
Uniting on the cyber challenge, and maintaining clear channels with global government bodies, helps inform and shape legislation.

**Enhance your capabilities.**
Our community is a trusted forum to share insights and learn from one another. Formal activities — like exercises and workshops — and informal relationship-building cultivate this trust.
How to get involved

If you see something...

Although Auto-ISAC is not a coordinated disclosure or bounty-based organization, anyone can submit information to Auto-ISAC. To submit vehicle cyber intel, email us at analyst@automotiveisac.com.

Join as a Member

If you are an OEM, supplier or commercial vehicle company, contact our Program Manager, Alexandra Heckler at heckler_alexandra@bah.com.

Partner with us

Individuals, vendors, researchers, government, academia, and others working in the connected vehicle ecosystem, contact Alexandra Heckler at heckler_alexandra@bah.com to learn about opportunities to engage.
Our contact info

Faye Francy
Executive Director

Booz Allen Hamilton Inc.
901 15th Street Northwest
Washington, DC 20005
703-861-5417
faye.francy@automotiveisac.com

Alexandra Heckler
Program Manager

Booz Allen Hamilton Inc.
901 15th Street Northwest
Washington, DC 20005
202-340-8308
heckler_alexandra@bah.com

Josh Laredo
Intel Coordinator

Booz Allen Hamilton Inc.
901 15th Street Northwest
Washington, DC 20005
617-538-1611
analyst@automotiveisac.com