CYBER RATINGS
FOR THE AUTO INDUSTRY:
SUMMARY OF KEY ISSUES

Jake Olcott, Vice President, BitSight Technologies
Key Questions at RSA 2016

1) Can cyber vulnerabilities in automobiles be exploited to cause harm to drivers?

1) How can auto manufacturers secure the vast vendor supply chain (e.g. telematics, software applications, etc.)?

1) How are auto manufacturers working to address these problems?

1) Are consumers aware of risks? How important is security to consumers? How do auto manufacturers provide information/assurance to consumers?
Impressions of Consumers in 2015

- 72% aware of Jeep hacking incident
- 41% say they will consider hacking when buying/leasing next car
- 78% say hacking will be frequent problem next 3 years
- 81% think auto manufacturer is most responsible to secure from hacking
- 64% want to go to dealership to get security patch installed

*From Kelley Blue Book Car Hacking Survey, 2016*
Only 26% could recall an instance of vehicle hacking

73% believe hacking will be a moderate/serious problem in the future

Millenials least likely generation to think vehicle hacking will be a problem over next 3 years (50% v. 70% of overall)

Top safety concerns “right now” – vehicle hacking #9 (out of 10)

Majority of millenials (60%) support more connected vehicles (v. 42% of total)

56% of consumers think vehicle manufacturers should be responsible for anti-hacking software

*From Kelley Blue Book Car Hacking Survey, 2016
Consumers Willing to Pay for Security

- 48% would pay for software to prevent vehicle hacking ($8.98/month)
- 56% would pay for additional insurance to cover hacking ($9.31/month)
- Millennials will pay more for software ($10.67) and insurance ($15.20)
Industry and Government Initiatives

- Bug bounties and crowdsourced vulnerability disclosure
- Auto ISAC – created to be central intelligence hub
- Hackathons
- NHTSA Automotive Cybersecurity Research Program
Sen. Markey SPY Act

- Response to Sen. Markey’s Tracking and Hacking: Security & Privacy Gaps Put American Drivers at Risk
- Requires “reasonable measures” to prevent car hacking
- Designs to isolate critical systems
- Transparent cyber “dashboard” that displays an evaluation to inform consumers about measures
- Involves NHTSA (vehicle safety) and FTC (privacy information)
Panelist Opinions: Generally

- Safety of the auto is paramount – (durability and safety are 2 most important decisions when purchasing car)
- Many similarities between vehicles and medical devices, where there are also natural regulators to play a role
- Crash test ratings developed as a result of NHTSA and insurance industry interest in enhanced design security
- Current crash test ratings do not factor cyber
- Unique cyber rating may be less preferred to incorporation of cyber into overall crash test assessment (though difficult to do)
- Insurance likely driver for enhanced cybersecurity in cars and supply chain
Panelist Opinions: The Dashboard

- Overall cyber maturity model – a systematic methodology to evaluate the hardware, software, supply chain security initiatives used by the manufacturer to build the car
- Vulnerability assessment (judged by independent third party?)
- Software development process – how code was written, acquired, tested, and deployed in the system
- Information about the security of the vendor supply chain, including 3rd party telematics vendors, software providers, etc.
- Patching system – performed remotely or on site?
# About BitSight Technologies

Led by security and networking industry veterans from:

- Q1 Labs (IBM)
- Raptor (Symantec)
- Okena (Cisco)
- MIT
- Sun Microsystems
- McAfee
- Brix
- VeriSign
- Credit Suisse

## Prestigious investors

![NSF](image)
![Menlo](image)
![Flybridge Capital Partners](image)
![Globespan Capital Partners](image)
![Commonwealth Capital Ventures](image)

## Trusted by customers, partners and independent standards bodies

![AIG](image)
![KKR](image)
![PwC](image)
![Deloitte](image)
![CEB](image)
# Bitsight Security Ratings

A Burgeoning Standard for Enterprise Risk Management

<table>
<thead>
<tr>
<th>Regulatory Impact</th>
<th>Enterprise Adoption</th>
<th>Industry Recognition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Briefings with top regulators</strong></td>
<td><strong>300+ Enterprise Customers</strong> worldwide and across all major industries</td>
<td>Recognized by leading technology research firm as a Cool Vendor 2015 in Vendor Management</td>
</tr>
<tr>
<td>including federal and state regulators in finance, energy, consumer</td>
<td><strong>8 top cyber insurers</strong> use BitSight to make underwriting decisions</td>
<td>Gartner: BitSight is “well on its way to being as widely recognized as a Moody’s or S&amp;P ratings for the information security space.”</td>
</tr>
<tr>
<td><strong>Active communication</strong> with important regulatory organizations including the Fed, OCC, FDIC and SEC</td>
<td><strong>3 of the top 5 investment banks</strong> use BitSight Security Ratings for VRM</td>
<td>Coverage in leading publications including the Wall Street Journal, Bloomberg, Forbes, etc.</td>
</tr>
<tr>
<td><strong>Working with financial services industry leaders</strong> to integrate Bitsight Ratings with SOC 2 evaluations</td>
<td><strong>4 of the top 5 private equity firms</strong> endorse BitSight</td>
<td></td>
</tr>
<tr>
<td><strong>Participant in standard setting groups</strong> including Shared Assessments and FS-ISAC</td>
<td><strong>2 of the Big 4 Accounting firms use BitSight</strong> - One firm has attested to the ratings methodology</td>
<td></td>
</tr>
</tbody>
</table>
Trusted by 300+ Enterprises
# BITSIGHT MARKETS

BitSight Security Ratings are used by companies in all industries to:

<table>
<thead>
<tr>
<th>Benchmark Security Performance</th>
<th>Manage Third Party Risks</th>
<th>Underwrite Cyber Insurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Compare security performance</strong> to industry averages and peers</td>
<td>• <strong>Continuously monitor</strong> security performance of third party vendors</td>
<td>• <strong>Better understand</strong> security posture of applicants and insureds</td>
</tr>
<tr>
<td>• <strong>Remediate threats</strong> facing your company</td>
<td>• <strong>Gain knowledge</strong> on your information supply chain weaknesses</td>
<td>• <strong>Monitor portfolio</strong> for possible changes in performance</td>
</tr>
<tr>
<td>• <strong>Communicate metrics</strong> to decision makers</td>
<td>• <strong>Screen new vendors</strong>, business partners, or acquisitions for security performance</td>
<td>• <strong>Bring actionable metrics</strong> into the underwriting process</td>
</tr>
</tbody>
</table>
COMPANIES ARE RATED ON A SCALE OF 250-900

HIGH RATING INDICATES A STRONG SECURITY PERFORMANCE AND LOWER SECURITY RISK

ANALYZES, RATES, AND MONITORS COMPANIES’ SECURITY PERFORMANCE, ALL FROM THE OUTSIDE

DAILY RATING AND ALERTS PROVIDE CONTINUOUS VISIBILITY
Generating Security Ratings

Output: Daily, outside data collection, quantitative ratings of a company’s security performance on a scale of 250-900
An analysis of 27,458 companies demonstrates that companies with a ratings of 500 or below are five times more likely to have experienced a publicly disclosed breach.

Statistical results replicated and verified by AIR Worldwide (leading insurance cat modeling)