RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: HT-T11

Braking the Connected Car: The Future of Vehicle Vulnerabilities

Karl Brauer

Senior Director
Automotive Industry Insights
Kelley Blue Book

Akshay Anand

Manager
Commercial Insights
Kelley Blue Book

#RSAC

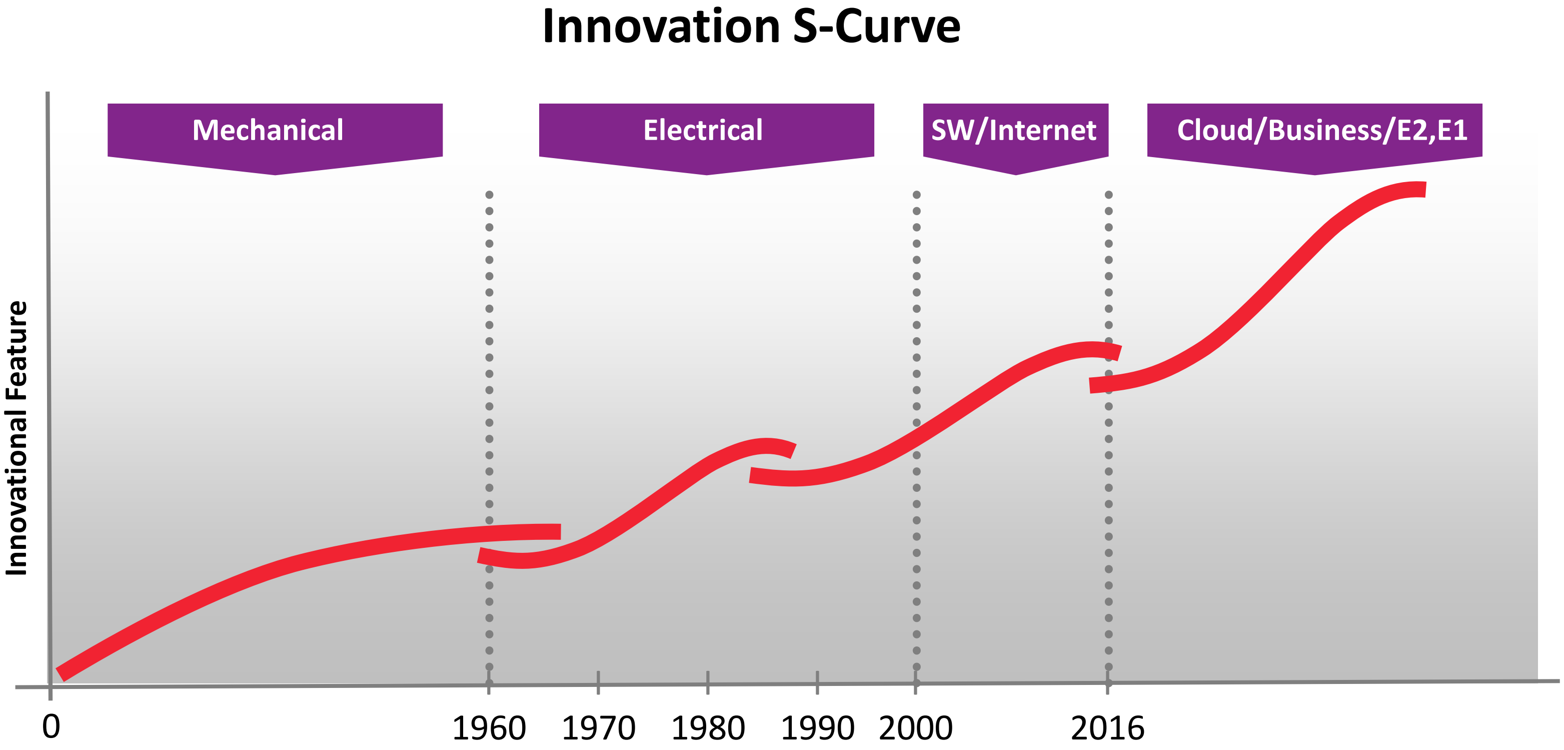
Vehicle hacking & the “Hindenburg Moment”

Happens whenever technology takes a leap forward

- Cars already becoming connected
- Cars will be autonomous in 5 years
- Vehicle hacking almost inevitable

Not yet worried about vehicle hacking? You should be.

Innovation S-Curve & "The Slip"



Topics that will be addressed today

- Examples of high-profile hacks and the variance in techniques (remote access, physical access and through supporting mobile phone software)
- A high-level analysis of Kelley Blue Book research to illustrate vehicle hacking vulnerabilities and consumer perceptions
- A future-casting of how in-car technology will evolve over the next 10 years with a focus on the potential to hack multiple devices (mobile phones, wearables, etc.) by hacking a car, or vice versa
- Mitigating risk by providing incentives for security researchers to share their vulnerability findings

Hacking is becoming a bigger issue, period

There were several high-profile hacks in 2015

"Anthem says hack may affect more than 8.8 million other BCBS members"

"One of the biggest security firms in the world admits it was hacked"

"Ashley Madison hack is not only real, it's worse than we thought"

"Hack brief: Hackers steal 15M T-Mobile customers' data from Experian"

"OPM hack: Government finally starts notifying 21.5 Million victims"

There are more vehicle hacking entry points than ever before

"FCA issues Uconnect software update amid hacking fears"

"OnStar hack remotely starts cars, GM working on a fix"

"Hacker uses smartphone to hack a connected car"

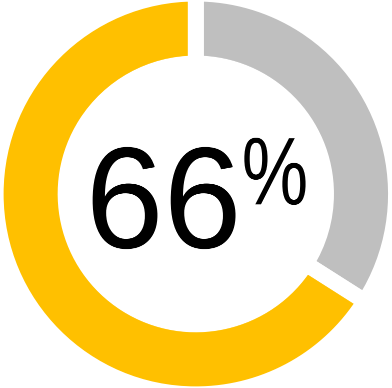
"Two researchers said they were able to take control of a Tesla Model S by hacking into the car's entertainment system"

"Hackers cut a Corvette's brakes via a common car gadget"

Kelley Blue Book
KBB.COM
The Trusted Resource

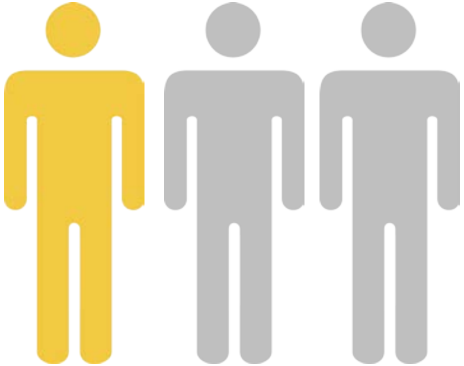
And technology is a make-or-break factor for many consumers – but with technology comes potential issues

When Choosing The Car I Will Purchase



Any Technology That Comes in the Car is an Added Bonus

1 In 3 People



Technology Features in the Car Will Make or Break My Decision

Q: When choosing the car I will purchase… In-Vehicle Technology Survey, August 2015 (N=2076)

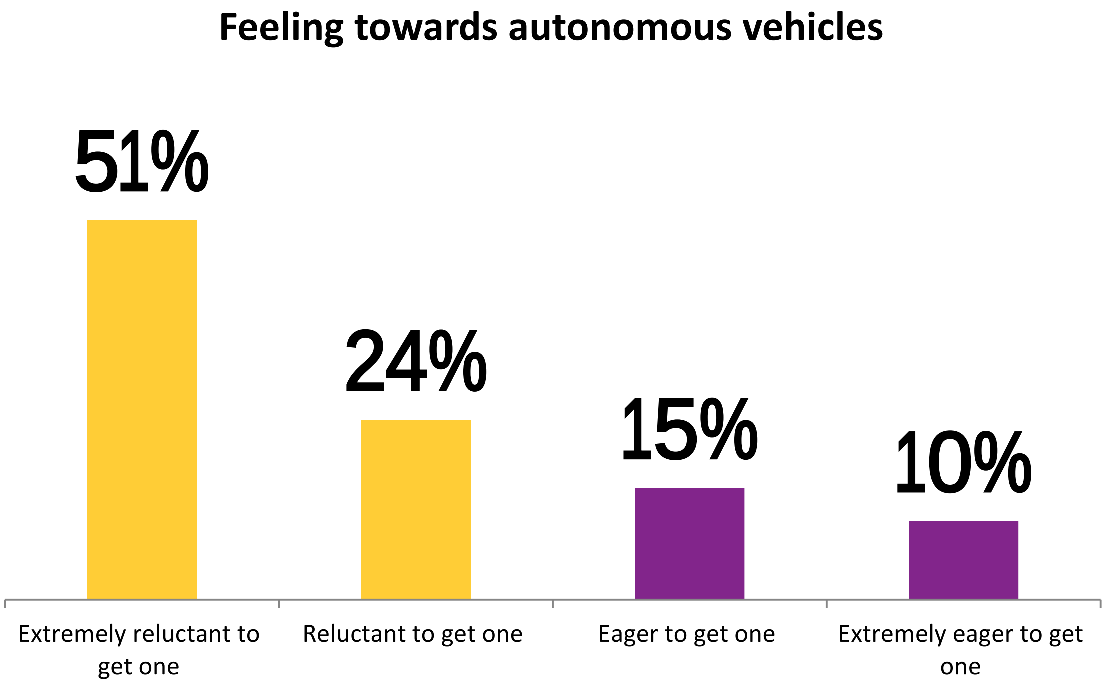
Over 40 % of consumers support connected vehicles – this number jumps for Millennials

42% **support vehicles becoming more connected**

Millennials are more supportive of vehicles becoming more connected vs. other generations. For example, the majority (60%) are supportive!

Q: How do you feel about vehicles becoming more connected, basically the "Internet on Wheels"? Vehicle Hacking Vulnerability Survey, January 2016 (N=813)

But as of now, most consumers are hesitant about autonomous vehicles, though we expect this to change in the future

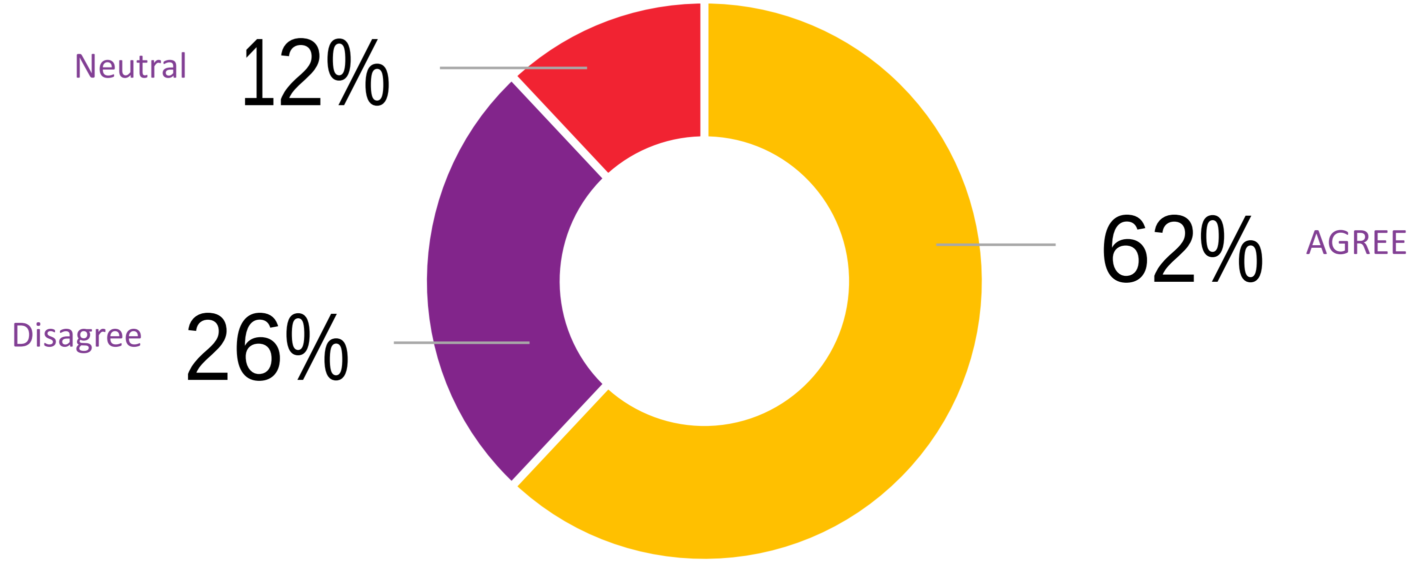


Q: How do you feel about autonomous or self-driving vehicles? Vehicle Hacking Vulnerability Survey, January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

As such, most consumers are worried about cars being hacked in the future

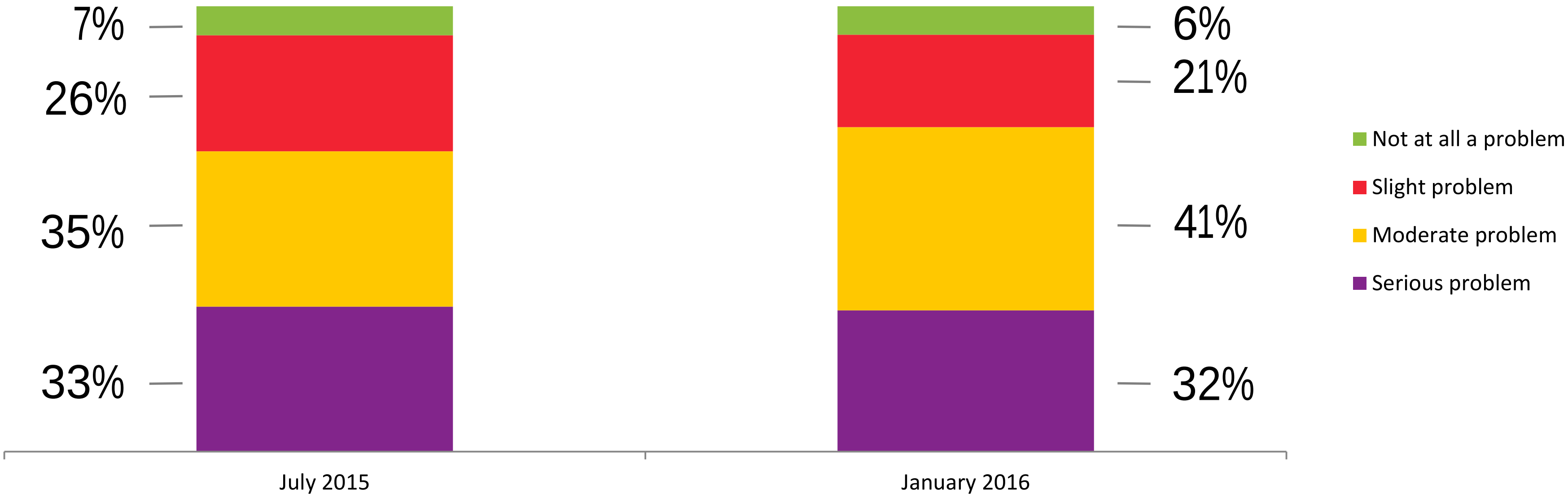
I Fear Cars in The Future Will Be Easily Hacked



Q: I fear cars in the future will be easily hacked. In-Vehicle Technology Survey, August 2015 (N=2076)

And well over half of consumers think hacking will be a moderate or serious issue in the future

Vehicle hacking in the future

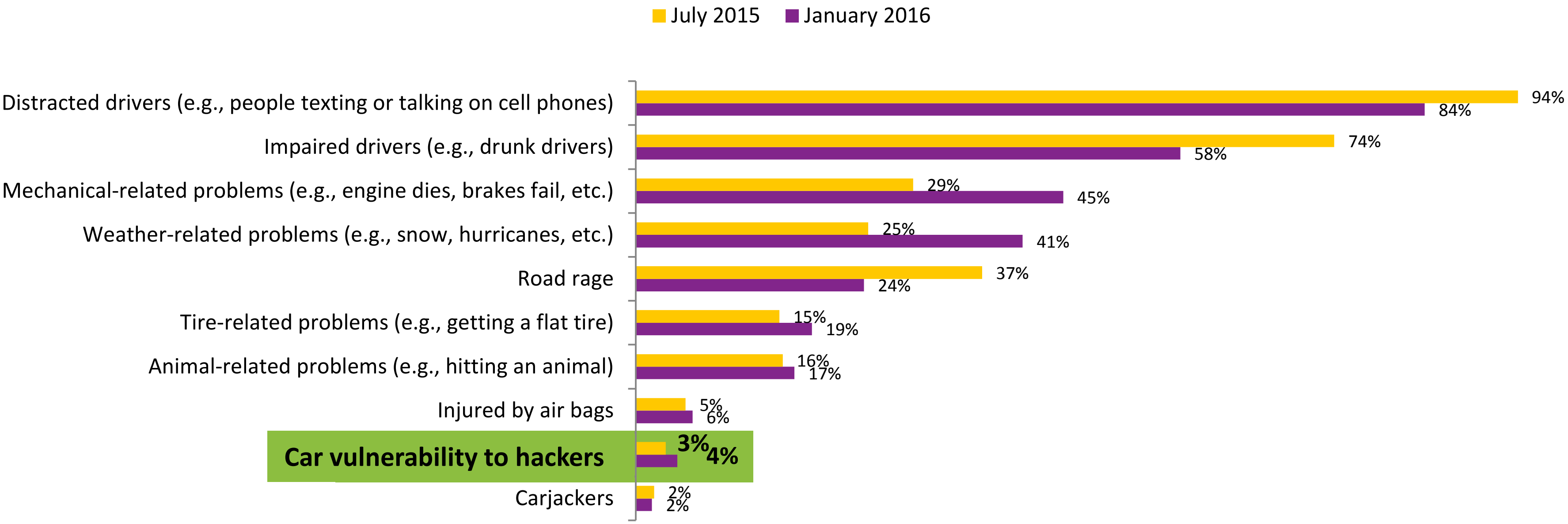


Q: How big of a problem do you feel vehicle hacking will be in the future? Vehicle Hacking Vulnerability Surveys, July 2015 (N=1134) and January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

While concerns about future hacking exist, consumers don’t list hacking as a top safety concern right now

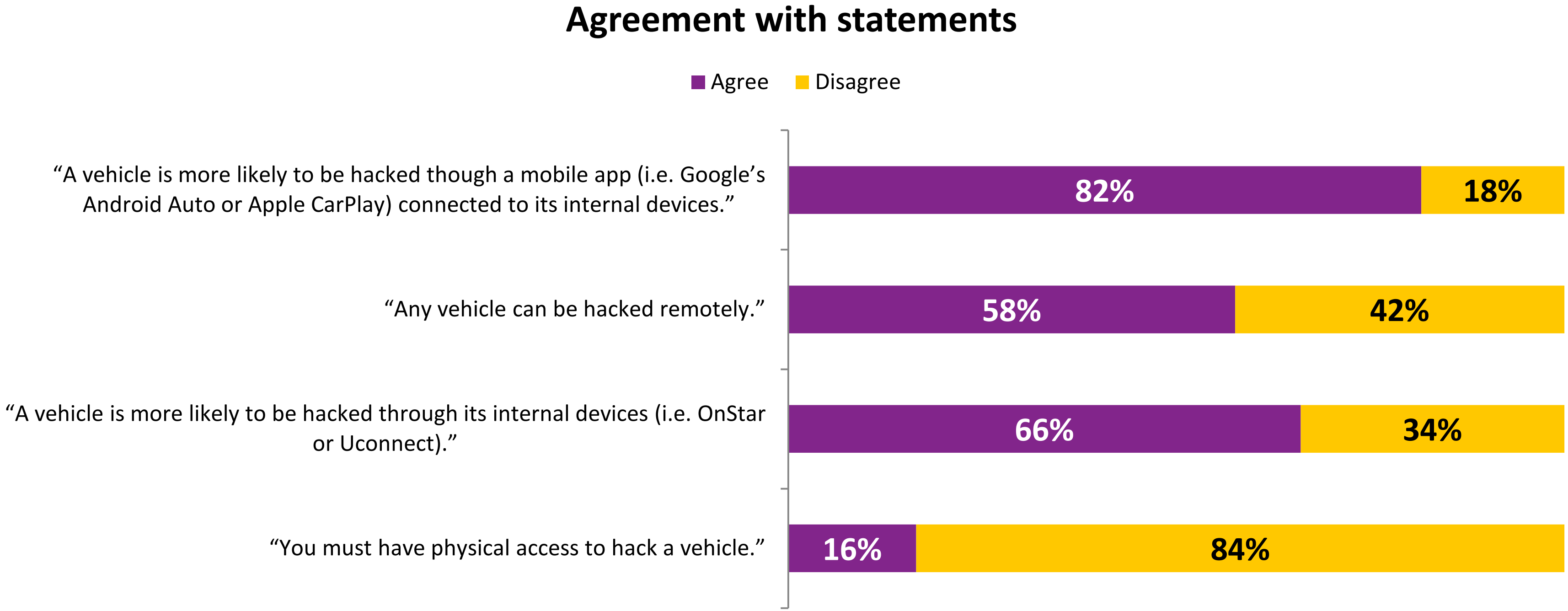
Top 3 safety concerns while driving a vehicle



Q: Based on the list below, what are your top 3 safety concerns while driving a vehicle? Vehicle Hacking Vulnerability Surveys, July 2015 (N=1134) and January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

Even though consumers are aware of the ability to be hacked through mobile apps, most wouldn't be willing to sacrifice the convenience factor

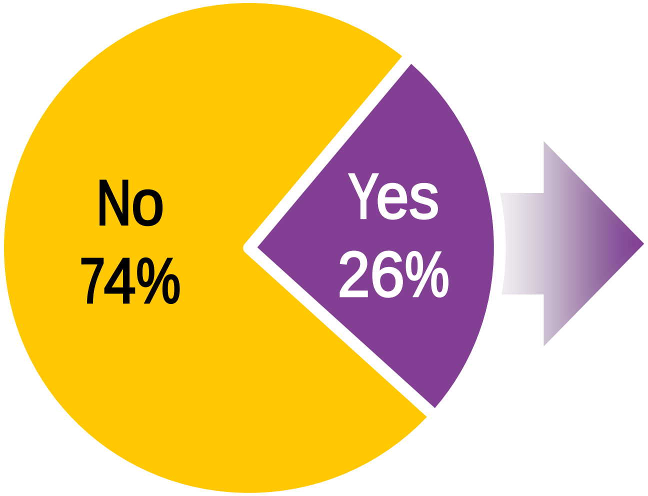


Q: To what extent do you agree or disagree with the following statements…? Vehicle Hacking Vulnerability Survey, January 2016 (N=813)

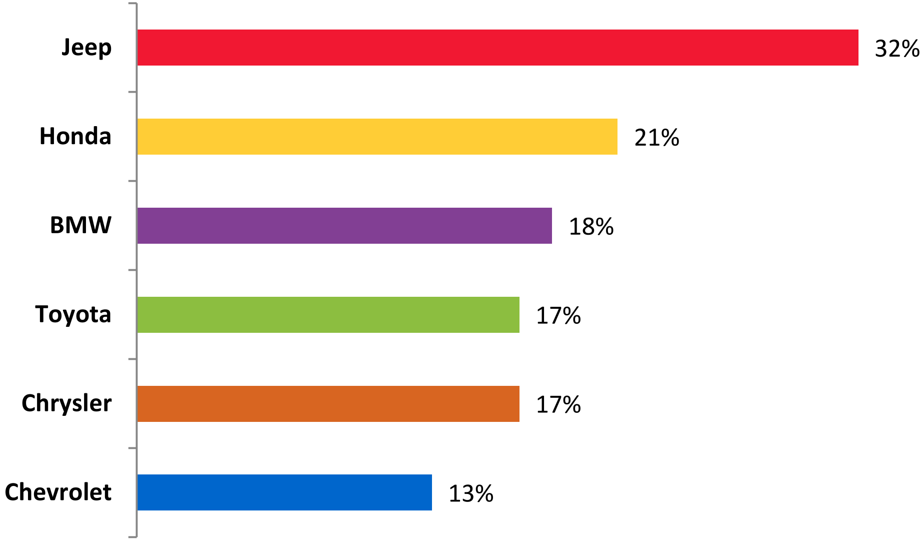
Despite the potential threats, consumers still throw responsibility elsewhere

Awareness of the Jeep hacking incident has dropped

Aware of any vehicles being hacked in the past year

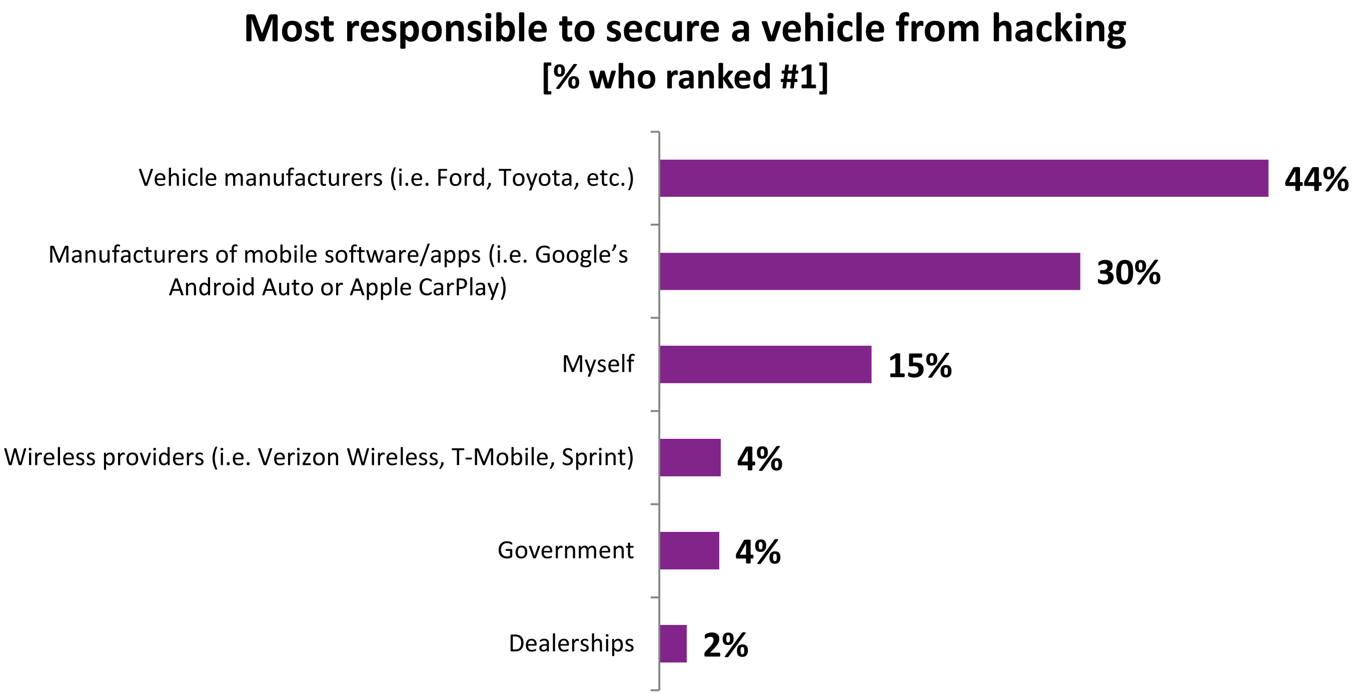


Brands you are aware of that were hacked [Top 5 listed]



Q: Are you aware of any vehicles being hacked in the past year? If so, which of the following brands are you aware of that were hacked in the past year? (Select all that apply.)
Vehicle Hacking Vulnerability Survey, January 2016 (N=813)

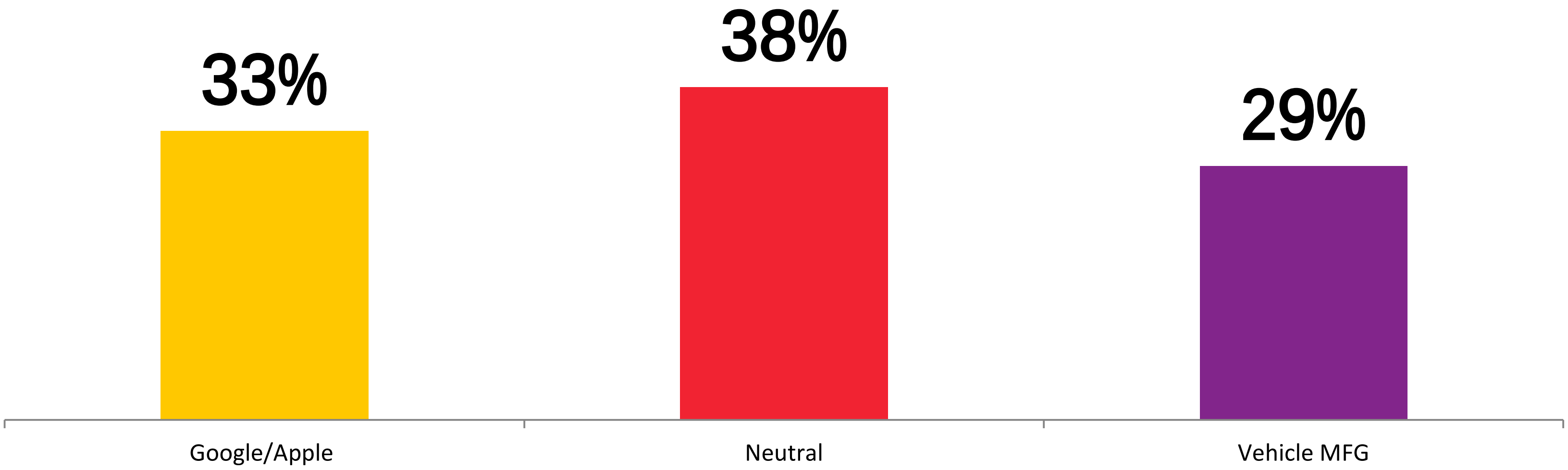
Consumers feel the vehicle manufacturer is most responsible for securing a vehicle from hacking



Q: Who do you think is responsible to secure your vehicle from hacking? (Please rank in order of responsibility with 1 being most responsible.) Vehicle Hacking Vulnerability Survey, January 2016 (N=813)
)

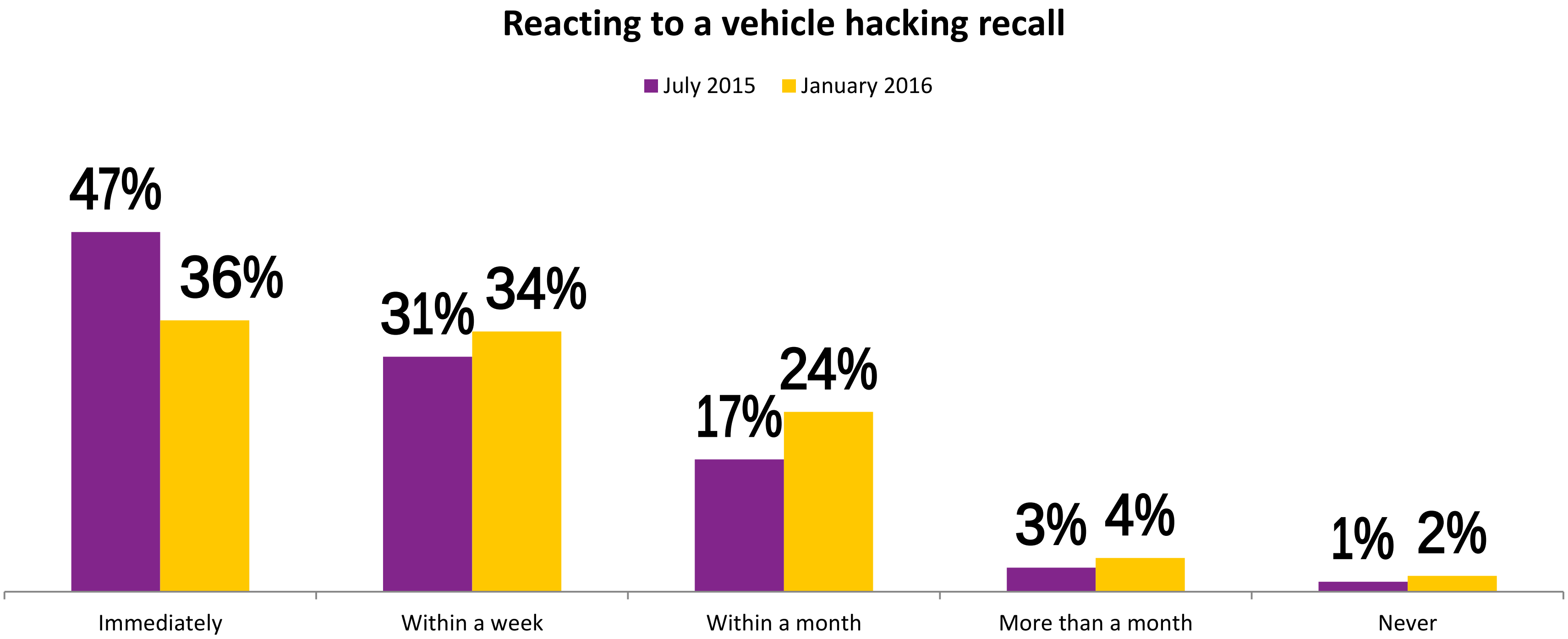
Consumers still view vehicle manufacturers as partially responsible even if hacked through a mobile phone!

Responsibility if vehicle is hacked through mobile phone software/apps



Q: If a vehicle manufacturer is supporting Google or Apple's mobile phone software/apps in a particular vehicle, who should be held more responsible if that vehicle is hacked? Vehicle Hacking Vulnerability Survey, January 2016 (N=813)

Almost half say they would bring their vehicle into a dealership immediately for hacking protection



Q: If you knew that you had to go into the dealership in order to install a security patch for your vehicle to protect from hacking, when would you do it? Vehicle Hacking Vulnerability Surveys, July 2015 (N=1134) and January 2016 (N=813)

So where are we currently and what’s next?

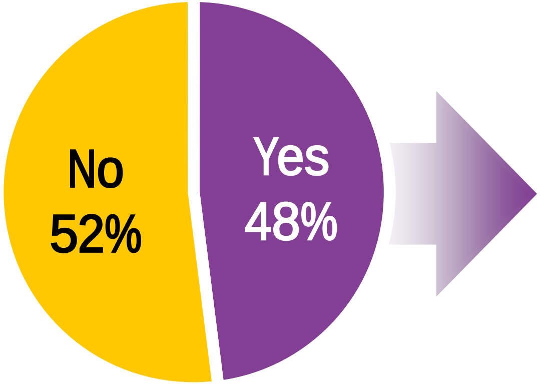
Current and future landscape…

Current

- Average car on the road is over 11 years old, so most cars currently remain unconnected
  - “Dumb” cars can, however, become connected as a result of aftermarket additions
- To our knowledge, no vehicle hacks have occurred in a non-controlled environment
- Most autonomous features are **driver-assist** vs. fully autonomous
- While the financial gains for hacking remain unclear at this point, the potential exists in the future (through ransomware, etc.)
  - Adversarial gains are possible

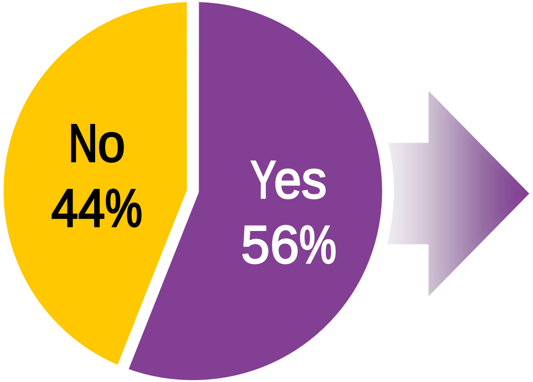
A decent chunk of consumers are in fact willing to pay for anti-hacking software

Pay for software that would prevent vehicle hacking (i.e. an antivirus)



Monthly subscription (mean) = $8.98

Pay for insurance to cover any losses incurred by vehicle hacking

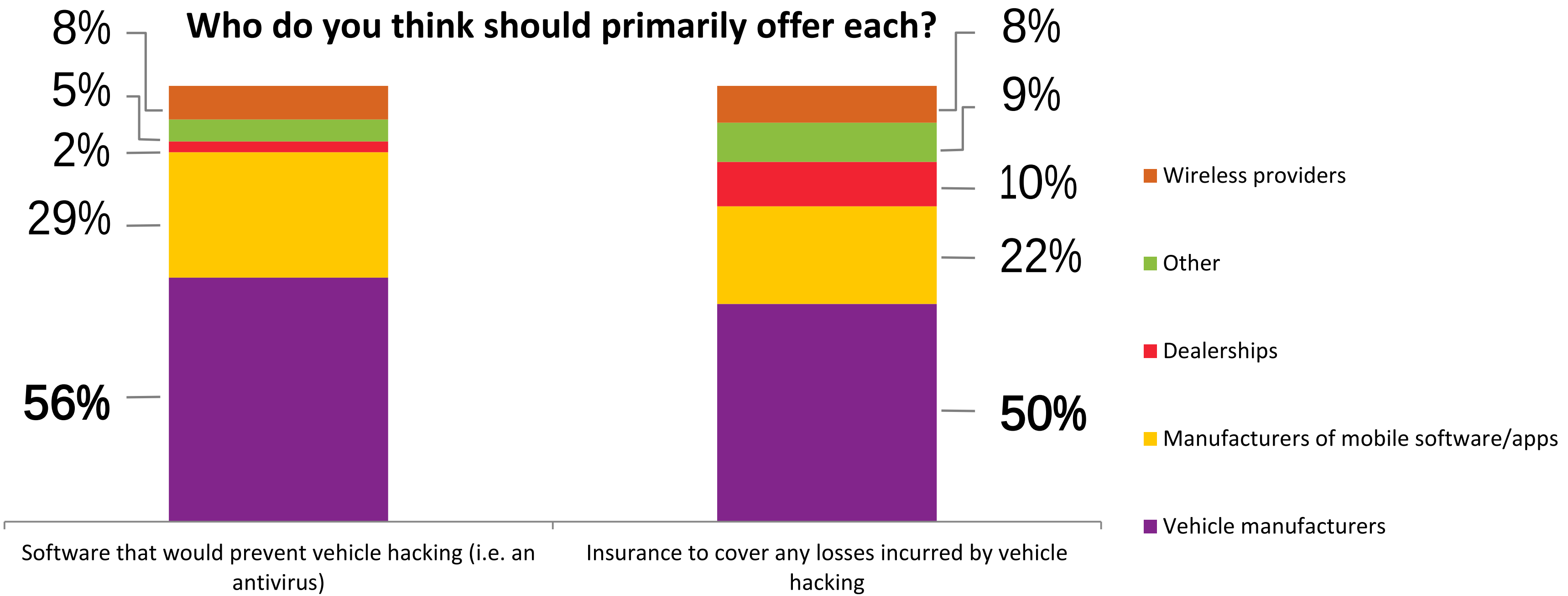


Monthly subscription (mean) = $9.31

Q: Would you pay for a monthly subscription for each of the following…? If so, how much would you pay for each? Vehicle Hacking Vulnerability Survey, January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

And consumers feel vehicle manufacturers should offer these subscriptions



Q: Who do you think should primarily offer each? Vehicle Hacking Vulnerability Survey, January 2016 (N=813)

Kelley Blue Book
KBB.COM
The Trusted Resource

Cars are becoming connected at a rate which will only increase

Vehicle Models with Internet Access

	2011	2012	2013	2014	2015	2016
Vehicles with Internet Access as STANDARD	2	14	53	89	151	133
Vehicles with Internet Access as OPTIONAL	1	10	37	67	93	69
Vehicles WITHOUT Internet Access	369	359	346	323	291	173

Source: Kelley Blue Book® Insights data

Kelley Blue Book
KBB.COM
The Trusted Resource

The future landscape – everything is connected!

Future

- Volkswagen BUDD-e – Mobile device on wheels
- Internet of Things connections to home, phone, work and infrastructure
- Potential to become a new form of cyberterrorism
- Difficult for consumers to know if a car has been hacked (if they're not paying attention)

Kelley Blue Book KBB.COM The Trusted Resource

Next Steps

Applied – How to get ahead of this issue

- Consumers' vigilance whenever connected with any device, including phone, IoT devices *and* car
- We are all assuming a certain level of risk for convenience
- Automakers should (if they haven't already):
  - Develop research teams
  - Crowd source vulnerabilities & collect information on every hack
- Government only now focusing on this issue
  - The process to create a standard is slow, however basic standards *do* need to be established similar to existing standards for crash tests, fuel efficiency, etc.
- The tech industry and automakers need to work **together** instead of viewing each other as competitors in regards to connected vehicles

What manufacturers and organizations are doing NOW to mitigate risks

- Tesla – cash for those who find vulnerabilities
- NHTSA – partnering with automotive and research firms to understand more about exploits, etc.
- Auto ISAC (Information Sharing and Analysis Center) – created by automobile OEMs as a central hub for intelligence analysis
- Hackathons such as Battelle-SAE CyberAuto Challenge, Black Hat, etc.

Thank You!

Karl Brauer

Senior Director
Automotive Industry Insights
Kelley Blue Book

Akshay Anand

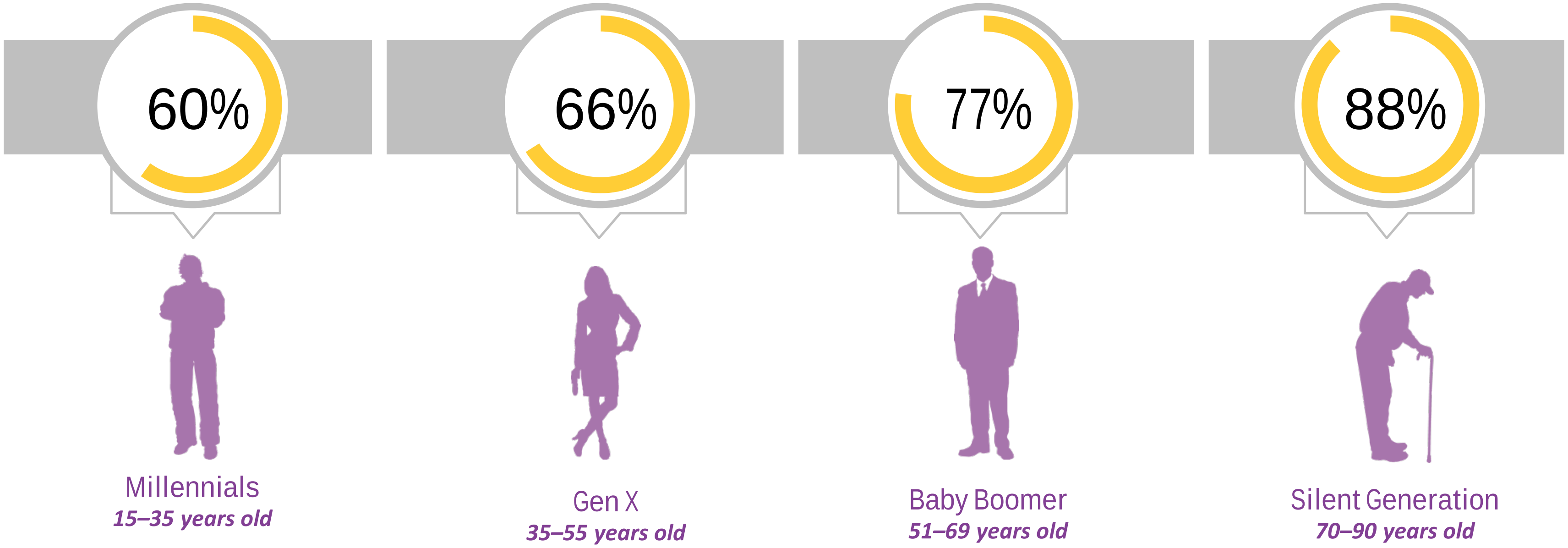
Manager
Commercial Insights
Kelley Blue Book

Appendix

Research conducted by Kelley Blue Book Strategic Insights between July 2015 and January 2016

Baby Boomers and the Silent Generation do not believe they'll own a self-driving car

Will You Ever Own A Self-Driving Car?



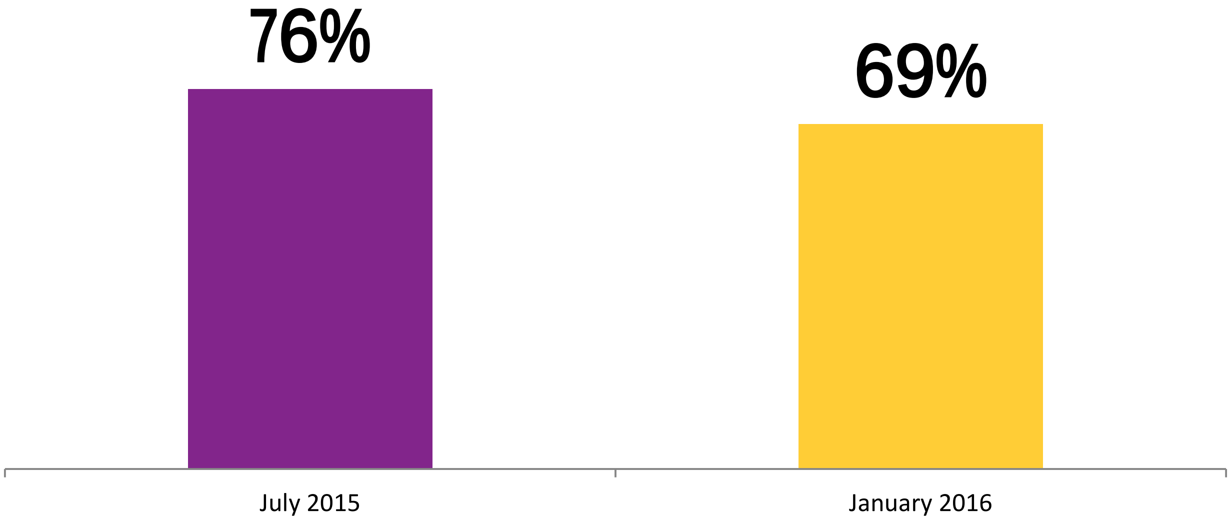
● No

Q: Will You Ever Own A Self-Driving Car? Q: What is the primary reason you don't think you will own a self-driving car? In-Vehicle Technology Survey, August 2015 (N=1552)

Kelley Blue Book KBB.COM The Trusted Resource

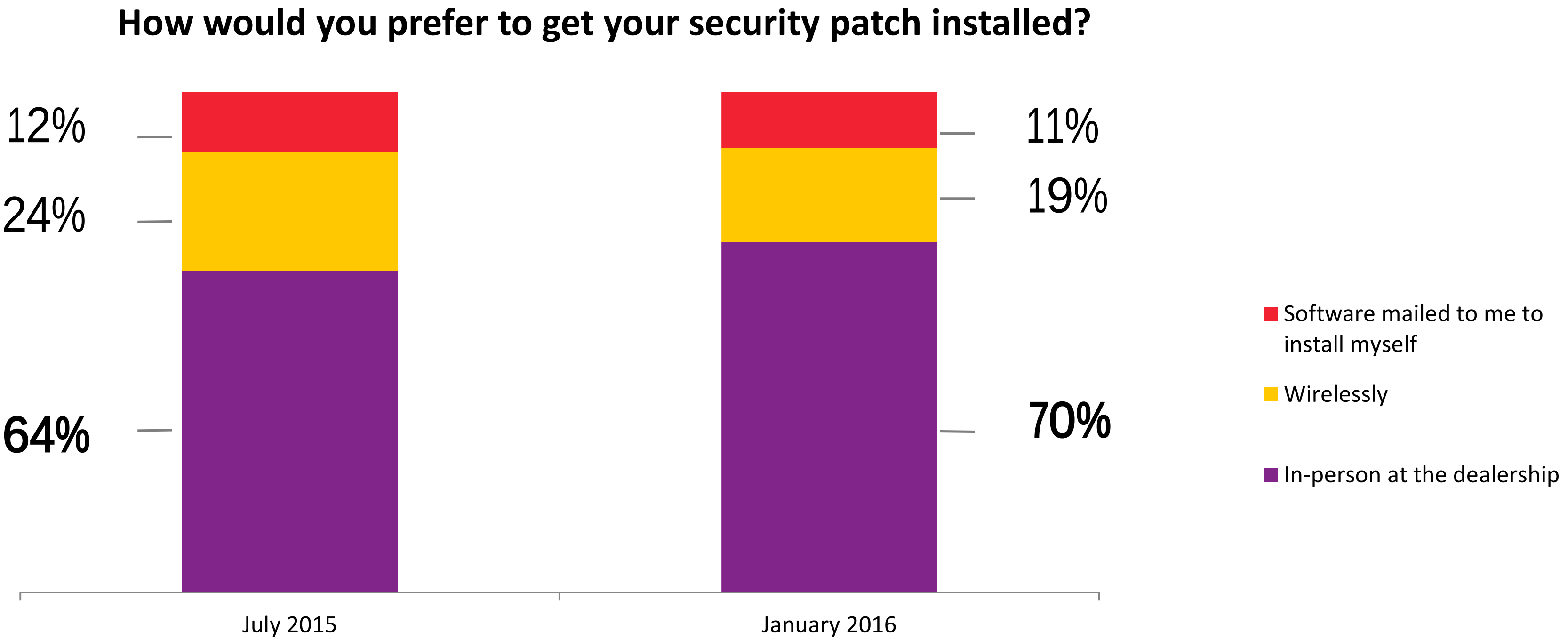
Majority think vehicle hacking will be a frequent problem within the next 3 years

Timeframe when vehicle hacking will be a frequent problem [Within the next 3 years]



Q: In what timeframe do you think vehicle hacking will be a frequent problem? [% who indicated “Right now” to “Within the next 3 years]
Vehicle Hacking Vulnerability Surveys, July 2015 (N=1134) and January 2016 (N=813)

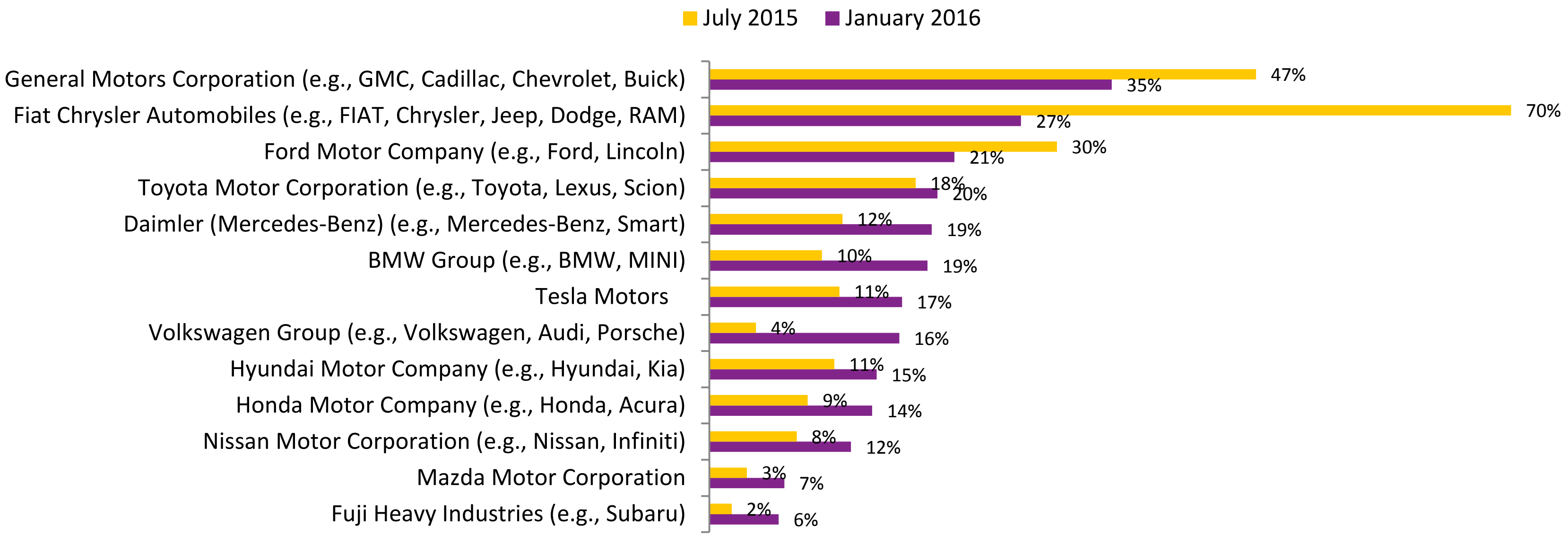
"In-person at the dealership" would be the preferred method to get a security patch installed



Q: How would you prefer to get your security patch installed? Vehicle Hacking Vulnerability Surveys, July 2015 (N=1134) and January 2016 (N=813)

NOTE: In January's survey, we did not mention the Jeep vehicle hack specifically by name

Auto MFG companies with vehicles that are more susceptible to hacking [You can select up to 3 answers]

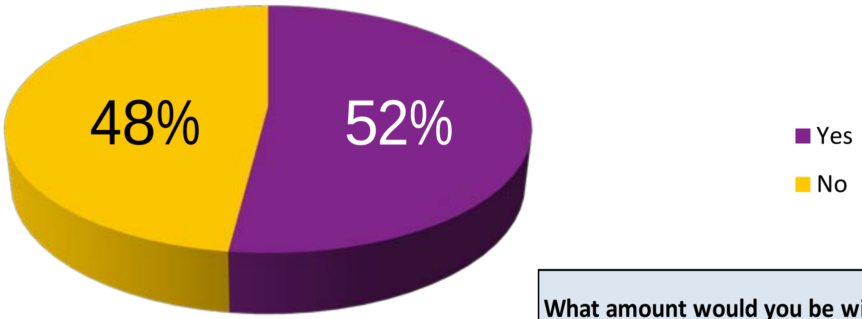


Q: Which of the following automobile manufacturing companies do you think have vehicles that are more susceptible to hacking? (You can select up to 3 answers.) Vehicle Hacking Vulnerability Surveys, July 2015 (N=1134) and January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

About half would pay a monthly subscription to completely protect their vehicle from hacking

Would you pay for a monthly subscription to ensure that your vehicle would be completely protected from hacking?



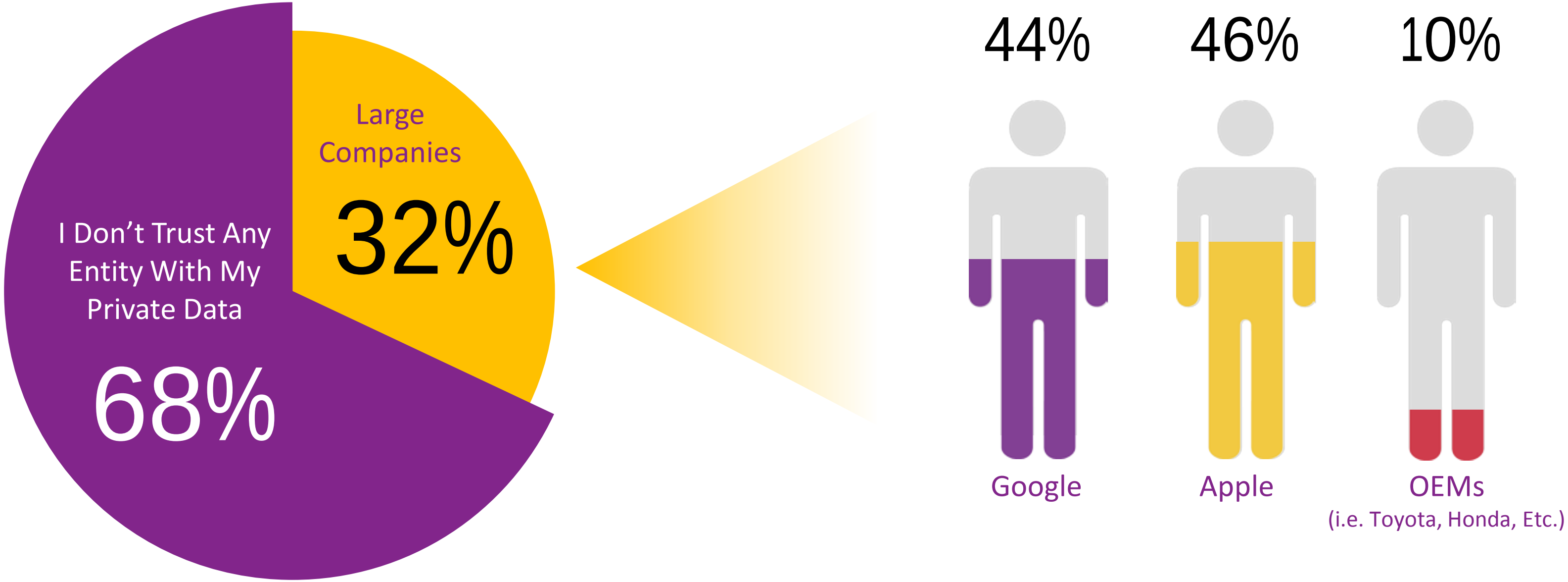
What amount would you be willing to pay? [N=591]	Monthly Subscription ($)
Monthly subscription amount - MEAN	$8
Monthly subscription amount - MEDIAN	$5

Q: If you had to pay for a monthly subscription to ensure that your vehicle would be completely protected from hacking, what amount would you be willing to pay?
Vehicle Hacking Vulnerability Survey, July 2015 (N=1134)

Kelley Blue Book KBB.COM The Trusted Resource

Consumers do not trust companies with their data

Who Do You Trust With Your Data?



Q: If the car you own has Android Auto or CarPlay (Apple's Infotainment system), who do you trust most with your data?
In-Vehicle Technology Survey, August 2015 (N=2076)

Kelley Blue Book KBB.COM The Trusted Resource