Luxury Daily®

The News and Intelligence You Need on Luxury

AUTOMOTIVE

# 80pc of consumers would be wary of automaker after data breach: report

July 27, 2016

*Audi Q3 mobility concept*

By FORREST CARDAMENIS

Nearly all consumers would be less likely to stay loyal to an automaker if it is hacked, according to the 2016 KPMG Consumer Loss Barometer study.



With connected and autonomous vehicles penetrating public consciousness, fear of cyber attacks not on automakers' data but on vehicles themselves has been the corollary. Despite public worries and dangers, however, automakers are not sufficiently investing in cyber security.

"An attack can take many forms either against the vehicle, the auto manufacturer and/or the customers and their personal information," said Gary Silberg, KPMG automotive sector leader. "The first example, where a cyber-attack is carried out against the vehicle, has been demonstrated at hacker conferences the last couple years.

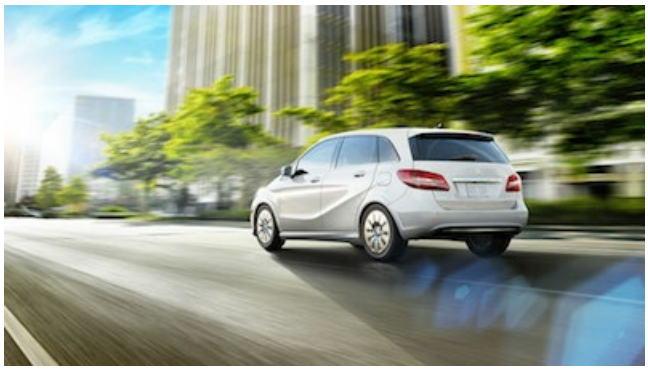
"In this scenario cyber actors can take remote control of a vehicle to kill the engine or control the air conditioning in a car," he said. "Last year research that showed this scenario is plausible caused one auto manufacturer to recall 1.4 million vehicles so they may have a cyber-security update installed to prevent the remote takeover of the vehicle."

"In the second example, auto manufactures and their suppliers are regularly targeted by cyber threat actors that are interested in stealing their intellectual property, merger and acquisition information, employee and customer data, banking data, hacking procurement and payroll systems. In short, they are targeting these corporations for anything of fungible value on the cyber underground or for wire transfer fraud.

"Hacking a vehicle or a retail corporation both require similar effort. To hack a vehicle, one would need to have knowledge of the systems in the vehicles. "

A blind eye

Seventy-nine percent of consumers say that if their car were hacked, the negative impact would be enough to dissuade loyalty to that automaker. These worries are largely geared at the future, as 51 percent say they are currently unconcerned about the possibility of their car behind hacked today, but that number drops to 30 percent when looking at the next five years.



*Mercedes electric B-Class 400*

Additionally, 10 percent of consumers say they would never buy from an automaker if that vehicle brand were hacked, with the share uniform across generations.

The jump in concern is attributable to the impending rise of connected, autonomous vehicles, with semi-autonomous vehicles already entering the market and some brands, namely BMW, promising the first self-driving automobiles as soon as 2021 (see story). With cars hooked up on a network, the prospect of a hacker taking over the vehicle concerns some consumers.

*BMW X5 hybrid*

While protecting these networks is its own task, consumers' cyber security concerns extend beyond the scenario. A quarter of consumers say theft of financial information is their biggest fear in a cyber attack.

Despite the concern from drivers, current statistics paint a picture of neglectful automakers.

In a survey of 100 automotive senior cyber security executives, 85 said their organization has been breached within the past two years, yet only 68 say capital funds have been invested in information security. Only 45 said someone at their company has an employee whose only job responsibility is information security.

*Jaguar F-Type Coupe*

Despite smaller consumer databases than large retailers, numbers point toward an increased fear of cyber attacks and much higher perceived potential damages in the auto sector.

As automakers publicize their vehicles of the future and the greatly improved safety of connected autonomous driving, they must ensure they are taking the new safety precautions that accompany these changes.

The cyber frontier

Concern surrounding cyber security is generally restrained to conversation about retailers. The volume of online shopping, as well as the frequency of data breaches, has led the industry to treat cyber security as a top priority.

As digital channels become increasingly important for retailers' businesses, cyber security has jumped to the top of industry insiders' lists of concerns.

A report from BDO released in May 2016 finds that 100 percent of retailers cite privacy concerns from a security breach as a worry, up from 55 percent in 2011. With highly publicized cases of hackers successfully sticking their hands in retailers' client data, the possibility of a potential break in security seems more realistic (see story).

The firm reactions some consumers say they will take in response to security compromises reflects the abundance of invisible costs that such attacks incur.

The costs most commonly associated with security compromises amount to less than 5 percent of the business impact, according to Deloitte Advisory.

While the fines, litigation fees and cost to improve cyber security are well-known expenses following a data breach, the loss of intellectual property, increase in insurance premiums and tarnished customer relations often equate to costs of a much higher magnitude. Taking a closer look at the associated costs of cyber attacks can help brands ensure they are properly budgeting security expenditures (see story).

"Cars and trucks have evolved into highly complex computers on wheels, with increased connectivity that presents cyber security risks, the most significant of which is safety," Mr. Silberg said. "Auto manufacturers and their supplies are now realizing the cyber risks.

"In response, they are building cyber security into their overall risk governance approach to ensure that the supply chain, design and manufacturing process and services have cyber security imbedded into the whole life cycle," he said. "In some cases they have even offered hacking bounties of thousands of dollars for anyone that can hack their vehicles.

"Automakers realize the threat is real and the implications of a vehicle breach could be disastrous both automakers and consumers alike."