PROPERTY CASUALTY 360°

Written BY John Sarich // November 2018

Weaponizing driverless cars

In an age of connected cars and cyber hackers, what could go wrong?

In the age of hacking, weaponized driverless cars pose compound liability risks. Considering all the technology built into driverless cars, it's not a big leap for anyone with an insurance mindset to think of the terrible ways it could go wrong

Hackers are moths drawn to the flames of digital systems. From the hacker's point of view, the more complex the system – and the more social disorder it's possible to create – the better. Think of the mega-hacks at the credit bureau Equifax, where 143-million American accounts were compromised, or Yahoo, which reported breaches of every single one of its accounts in 2013 (upwards of 3 billion in total).

The hacked data-collecting technology noted above is kids' stuff compared with the complexity and artificial intelligence needed to power a driverless vehicle. With hacked cars, there is a real risk of losing lives, not just data privacy.

Weaponizing autonomous vehicles

We have not yet witnessed a drone-style capacity to control one or multiple vehicles remotely. Even so, too many tragic instances of cars being turned into weapons have already occurred. In one of many examples worldwide, a rental van in Toronto mowed down pedestrians on the sidewalk of a busy downtown intersection in April 2018, killing 10 people and injuring 15 others.

The deadly Toronto incident was not defined by authorities as a "terrorist" attack. But as the FBI notes in a 2010 report: "Vehicle ramming offers terrorists with limited access to explosives or weapons an opportunity to conduct a homeland attack with minimal prior training or experience." The potential for hacking fully-automated cars means that attacks could expand beyond just isolated incidents; there could be coordinated attacks multiplied over many geographies. The risk of fatality increases exponentially, with no risk of life to the hacker.

In a worst-case scenario, hackers operating domestically or remotely could program driverless cars to become autonomous missiles in the middle of big cities. Imagine the damage that could be done by figuring out how to disable the brakes on a moving driverless truck. Even if it's not taken this far, hackers could remotely disable one or multiple autonomous vehicles, causing pandemonium on a highway during rush hour; or they might shut down an entire fleet of self-driving delivery vehicles, which may at that moment be in multiple locations doing their job.

A Wall Street Journal report on hackable cars highlights the potential for other, comparatively tame acts of cybercrime. In "carnapping," for example, hackers could lock car owners out of their cars and demand a ransom for re-opening the doors. Enough of these digital lockouts would not only amount to a hefty sum in ransom money, but they could put a vehicle manufacturer out of business because of reputational and trust issues. While such a scenario is clearly not life-threatening, the potential to hack into fully-automated cars does raise the issue of insuring the risk.

Insurance and driverless cars

The safety benefits of driverless cars are sometimes touted as part of a discussion

within the Canadian property and casualty insurance industry. Between 1993 and 2016, there have been an average of 2,234 traffic-related deaths each year in Canada. South of the border, in the United States, there are nearly 36,000 traffic-related deaths every year; 94% of these tragedies are due to "human choice or error." Remove the factor of human choice, safety advocates say, and the crash rate goes down. Lives are saved. People don't get as angry or frustrated during their commute to work. Speeding tickets become a thing of the past. No more points on your licence — because you don't have a licence. All these wins for drivers are likewise a boon for insurers. Fewer collisions mean lower claims costs, and reduced auto liability losses.

All good stuff, right?

But what about the pedestrian in Arizona who was killed by an experimental Uber car driving in autonomous mode? Video suggests the human sitting in the driver seat was looking downward at the time. And what about all the other human drivers on the road who aren't content to drive behind an old-lady robot? The core of the insurance industry is to identify risks, quantify the exposures and price the risk appropriately. The risks associated with autonomous cars could take many forms, and include:

For the vehicle manufacturers:

- a loss of public trust and corporate reputation

For the human drivers:

- property loss
- personal injury
- personal liability for causing a collision, injury or death

For pedestrians

- property damage, personal injury or loss of life

These risks increase exponentially with the potential for hackers to turn these vehicles into weapons. Manufacturers developing autonomous vehicles need to understand the broader risks and do a deeper dive into the potential liabilities.

A parallel with Facebook and Twitter comes to mind. By connecting us through these platforms, social media has the power to do enormous good. However, during the origins of their evolution, it appears no one gave serious thought to how they could be misused by those who wish to do us harm. The same could be said for driverless cars. Without addressing the potential downsides, the risk is too great.

John Sarich is an industry analyst and vice president of Strategy at VUE Software. He is a senior solutions architect, strategic consultant and business advisor with over 25 years of insurance industry experience. He can be reached at John.Sarich@VUESoftware.com.

End of Article

Original Link: https://www.canadianunderwriter.ca/wp-content/uploads/2018/11/CU-20181101.pdf (Page 59- 60)

John Sarich, *Vice President of Strategy* VUE Software.

About VUE Software

VUE Software is an innovative provider of performance-driven solutions built exclusively for the insurance industry. With over twenty-three years of experience in Life & Annuities, Health and P&C Insurance, VUE Software is one of the most experienced and established Insurance Distribution Technology providers in the business today. VUE Software is leading the Distribution Modernization movement, bringing clients a solid path to revenue growth and competitive advantage.

Inc. 5000

Microsoft Partner
Gold Application Development

VUE Software is the product division of Computer Solutions and Software International, LLC. (CSSI). This Featured Article is for informational purposes only. CSSI MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. VUE Software and the VUE Software logo are either registered trademarks or trademarks of CSSI in the United States and/or other countries. All other trademarks are property of their respective owners.