DfT rolls out key principles to strengthen vehicle cybersecurity in the CAV industry

17/08/2017

TMT analysis: The government has released guidance in the form of eight key principles for cybersecurity for driverless cars. Lucy McCormick, a commercial barrister at Henderson Chambers, takes them for a test drive.

What has triggered the release of these key principles by the Department for Transport

The vulnerability of modern vehicles has been a concern for some time. Notoriously, in 2015, a pair of security researchers found a way to gain remote access to a Jeep Cherokee and take control of the engine, brakes and entertainment system—this prompted a recall of 1.4 million vehicles.

Manufacturers and governments are particularly concerned about the possibility that cars could be taken over in a 'ransomware' attack along the lines of the 'WannaCry' virus, which paralysed the NHS in May 2017. Equally, the possibility for terrorist incidents is obvious.

At a more mundane level, smart cars are capable of gathering a great deal of sensitive data, for example about how often users go to the gym or where they worship—it is important that this is safeguarded.

Against that background, it is understandable and timely that the Department for Transport (DfT) has chosen to give guidance about what it expects from the industry.

What do the principles cover?

The principles are intended for use throughout the automotive sector and its supply chain. The eight 'headline' principles are:

- organisational security is owned, governed and promoted at board level
- security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain
- organisations need product aftercare and incident response to ensure systems are secure over their lifetime
- all organisations, including sub-contractors, suppliers and potential third parties, work together to enhance the security of the system
- systems are designed using a defence-in-depth approach
- the security of all software is managed throughout its lifetime
- the storage and transmission of data is secure and can be controlled
- the system is designed to be resilient to attacks and respond appropriately when its defences or sensors fail

Do they go further than existing regulation in this area?

The eight principles are not 'regulation' as such—they have no statutory status. However, they are a useful pointer to what the DfT expects from the industry. Should a manufacturer fall short of these guidelines, it is likely that this would be taken into account in any negligence or corporate manslaughter proceedings. If these guidelines are not taken seriously, the government may become more heavy-handed and seek to legislate.

Lying behind the key principles are a wide range of applicable standards and guidance. For example, SAE International, a global association of engineers in the aerospace, automotive and commercial-vehicle industries, has issued 'J3061—the cybersecurity guidebook for cyber-physical vehicles systems'. The International Standards Organization has published at least a dozen codes which are relevant to the security of connected and autonomous vehicles.

How should organisations be approaching the adoption of the principles?

To a degree the principles are common sense, and many organisations in this sector will already be in compliance. In the first instance, the priority should be for organisations to consider these security issues at a board level, and from there to try to implement training to embed a 'culture of security' throughout their business and at each level of their supply chain. The principles encourage organisations to collaborate and engage with appropriate third parties—in other words there needs to be a 'joined up approach' throughout the industry.

Are there likely to be any obvious practical difficulties or challenges in the adoption of these principles by organisations?

Broadly speaking, the principles are all fairly attainable. Some overlap with previous guidance from government—for example Principle 3.4— 'organisations ensure their systems are able to support data forensics …to identify the cause of any cyber or other incident'—has echoes of the requirement in the July 2015 Code of Practice for testing driverless cars on public roads that vehicles have 'black box' style data recording to help determine the cause of any accident.

Some might see tension between principle 6.1 emphasising the importance of 'secure coding practices' and principle 6.4 promoting 'open design practices' and sharing source code where appropriate. However, this tension is more perceived than real—peer reviewed code is ultimately likely to be more robust.

The principle which is most likely to hit organisations in their wallet is 3.1, which sets out the expectation that 'organisations plan for how to maintain security over the lifetime of their systems, including any necessary after-sales support services'.

What comes next for the regulation of the connected and autonomous vehicles (CAV) industry? Are there any major differences between the proposed Autonomous and Electric Vehicles Bill and its predecessor—the Vehicle Technology and Aviation Bill?

The Autonomous and Electric Vehicles Bill has already been through several metamorphoses. In the May 2016 Queen's Speech, it was announced that a 'Modern Transport Bill' would be put forward, encompassing not only autonomous and electric vehicles, but also drones and spaceports. When the full draft Bill actually emerged, it had been renamed the 'Vehicle Technology and Aviation Bill' and made no mention of drones or spaceports. The Bill progressed no further due to the general election.

Following the general election, in June 2017 the Automated and Electric Vehicles Bill was announced in the Queen's Speech. From the briefing, this appears to be substantively the same as its predecessor in terms of provision for the CAV industry, but it is not possible to be sure until a full draft Bill is published.

Looking further forward, the government is looking at a wide range of reforms, notably at whether to update the Ministry of Transport test and driving test to accommodate 'driverless' technology.

Lucy McCormick is a commercial barrister at Henderson Chambers. She is a leading expert in CAV and the co-author of Law and Driverless Cars. She lectures nationally and internationally on the legal implications of this rapidly developing area, from both an insurance and a product liability perspective.

Interviewed by Devon Marshall.