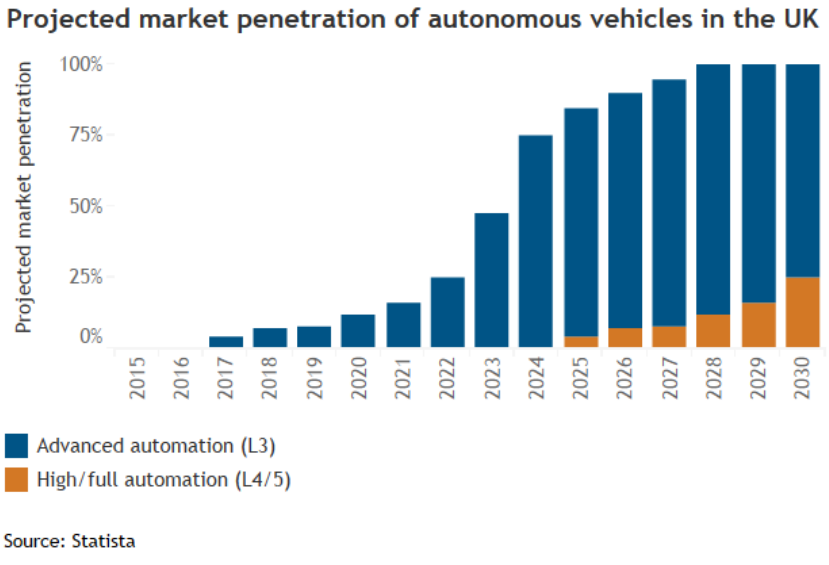
Cybersecurity regulation gets personal

Blog post by Practice Lead Conan Darcy, 31 August 2017

UK government proposals on cybersecurity in the automotive sector highlight how one unexpected outcome of digitisation could be the introduction of strict corporate governance rules previously unseen outside of the financial services sector.

Earlier this month, the UK government published its "key principles of vehicle cyber security for connected and automated vehicles", ahead of the Automated and Electric Vehicles Bill due to be tabled in the autumn, which is expected to focus on insurance regimes for driverless technology. The guidelines reflect the government's ambition for the UK to take a leading role in pioneering these new technologies and an acknowledgement that to do so requires establishing a robust and sophisticated regulatory framework.

The initial focus on cybersecurity is understandable. The growth of autonomous vehicle technology will connect previously unconnected vehicles and in turn create a multitude of new digital vulnerabilities for hackers, criminals, terrorists and hostile governments to exploit. Governments and their publics will need to be satisfied of the technology's security and safety before it can become a standard, let alone dominant, technology on road networks.



Source: Statista

One principle has unsettled some figures within the industry – that "personal accountability is held at board level for product and system security". In one sense, this proposal is a reflection of current scepticism in Whitehall that some corporates are not taking cybersecurity seriously enough, a perception compounded by high-profile examples of companies having delayed disclosing breaches, e.g. Yahoo. There is also a concern that many companies appoint senior figures to boards who lack digital acumen since this was not a major part of their experience as senior executives running businesses.

However, it also reflects a more fundamental shift in the seriousness with which regulators and policymakers are approaching cybersecurity regulation. The concept of "personal accountability" is well established in financial services, where it has been justified in terms of needing to protect financial stability and security. The consequence of digitisation for corporate governance policy looks to be in redefining the concept of regulatory "security" beyond financial security to also include cybersecurity and, in so doing, broaden the types of companies potentially subject to "personal accountability" frameworks – not just automotive but any future connected industry, e.g. energy.

In financial services, companies, executives and employees have complained that regulatory initiatives, such as the FCA's Senior Managers Regime, are overly personal and are designed to create scapegoats for public consumption. Others have pointed out that the strictness of such rules deter talented individuals from accepting senior appointments. We are likely to hear similar complaints and opposition from the automotive sector, though the fallout of the Volkswagen emissions scandal could dampen the effectiveness of these arguments. As the media, MPs and the public demand, post-financial crisis, more individual accountability from senior corporate figures, the question for the automotive sector is whether this battle has already been lost.

© Global Counsel 2017