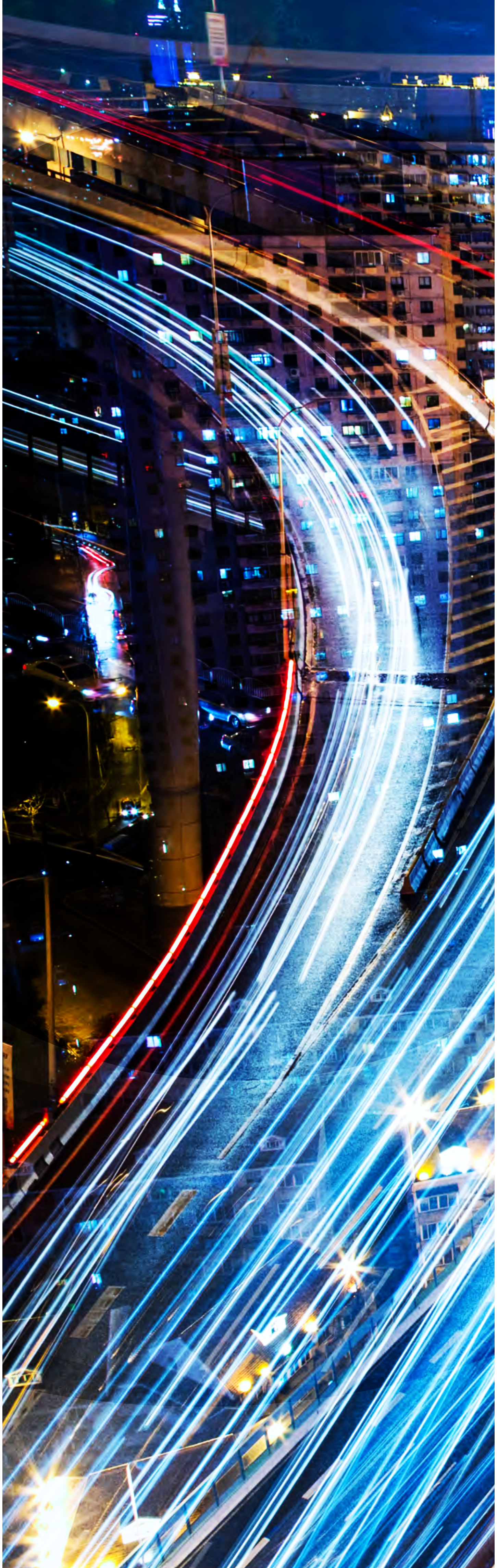
CONNECTED AND AUTONOMOUS VEHICLES: A HACKER'S DELIGHT?

CYBER SECURITY IN THE CONNECTED AND AUTONOMOUS VEHICLE INDUSTRY.

SEPTEMBER 2017

GOWLING WLG

UKAutodrive



CONTENTS

ABOUT UK AUTODRIVE

UK Autodrive is the largest of three UK consortia launched to support the introduction of self-driving vehicles in the UK. The aim of the consortium is to establish the UK as a global hub for the development of autonomous vehicle technologies and to integrate connected and autonomous vehicle technologies into urban environments.

UK Autodrive brings together leading technology and automotive businesses, forward-thinking local authorities and academic institutions to deliver a major three-year UK trial of autonomous and connected vehicle technologies.

Consortium members are Arup, AXA, Coventry City Council, Ford, Gowling WLG, Horiba Mira, Jaguar Land Rover, Milton Keynes Council, RDM Group, Tata Motors European Technical Centre, Thales, The Open University, Transport Systems Catapult, the University of Cambridge and the University of Oxford.

ABOUT GOWLING WLG

Gowling WLG is a Global 100 legal practice, with more than 1,400 legal professionals across 19 cities in the UK, Canada, Europe, Asia and the Middle East. Focused on key global sectors including automotive, tech, energy, infrastructure and real estate, they are able to provide clients with deep sector expertise.

Led by Stuart Young, the market-leading automotive industry group brings together technical excellence in regulatory, corporate, employment, dispute resolution, real estate, commercial and competition law.

It is the only law firm playing a significant role in the £19m UK Autodrive connected and autonomous vehicles programme, part of the UK government's driverless cars initiative.

METHODOLOGY AND OBJECTIVES

This is the third in a series of thought leadership reports about connected and autonomous vehicles (CAVs) produced by Gowling WLG on behalf of UK Autodrive. The Government wants the UK to become a global hub for the development of autonomous and connected vehicle technologies, and testing of CAVs in urban areas has already begun.

The threat of cybercrime is a reality for all of us. Whether you're the head of a large business or someone who only uses a device to update their Facebook status, a cyber-attack could affect you. In fact, recent Government statistics found nearly half of all UK businesses suffered a cyber breach or attack in the last year. In this report we explore what this means for connected and autonomous vehicles and how the industry is responding to the threat.

The research was conducted by BizWord Ltd (www.bizword.co.uk), an independent business consultancy.

Specific sources have been listed in the body of the report. To compile the report, we undertook in-depth interviews with a panel of experts including academics, industry specialists and representatives from the UK Autodrive consortium during May and June 2017. We also conducted desktop research and analysis of publicly-available information, industry studies and forecasts.

Many thanks to our contributors, for giving their time and sharing their expertise. They included:

- Anna Bonne, Head of the Transport Sector at the Institution of Engineering and Technology (IET).
- Professor Phil Blythe, Professor of Intelligent Transport Systems at Newcastle University and Chief Scientific Adviser, for the Department for Transport.
- Nadim Choudhary, Associate, dealing with Resilience, Security and Risk at Arup.
- Peter Davies, Technical Director at Thales e-Security.
- Peter Edwards, Chief Architect and Cyber Security Lead at Arup.
- Professor Martyn Thomas, CBE, Professor of IT at Gresham College.
- David Wong, Senior Technology and Innovation Manager at The Society of Motor Manufacturers and Traders (SMMT).

DEFINITIONS

AUTONOMOUS VEHICLE (AV)

A vehicle which is capable of fulfilling the operational functions of a traditional vehicle without a human operator.

CONNECTED VEHICLE (CV)

A vehicle which has technology enabling it to connect to devices within the vehicle, as well as external networks like the internet, allowing it to "talk" to its surrounding infrastructure and other vehicles.

CONNECTED AND AUTONOMOUS VEHICLE (CAV)

A connected and autonomous vehicle combines both sets of technologies' capabilities.

INTRODUCTION

Connected and Autonomous Vehicles (CAVs) are set to become part of the hyper-connected world we live in. To enable them to operate with little or no human input, they will use information from on-board sensors and from the surrounding digital environment to tell them where they are and what is around them.

As well as making the usual commute easier, these vehicles have the potential to benefit society both socially and economically. While individual vehicles will reach high levels of autonomy quite soon, they will struggle to deliver broader societal benefits unless they are effectively networked. It is the connected element of CAVs that turbo-charges those benefits, especially around reducing congestion and harmful environmental impacts.

Solo CAVs will be beneficial to their owner/users but traffic will need to move in a more coordinated fashion in order to maximise throughput.

But what are the risks associated with all this communication? Following a raft of recent, heavily publicised, global cyber-attacks aren't we simply opening another door for a malicious hacker? Is it possible or even feasible to make these new vehicles cyber resilient? And what does resilience mean in this context?

This report does not attempt to offer detailed technical solutions. Instead, it focuses on the nature of the cyber risk and discusses how the motor industry and our law makers need to react to the increased importance of all-things-cyber while they develop CAVs.

We hope you find the following pages thought-provoking and that they are a useful addition to the current debate.

> "Apollo 11, the spaceship that took humans to the moon, had 145,000 lines of computer code. The Large Hadron Collider has 50 million. The Android operating system has 12 million. A modern car has about 100 million lines of code."

STUART YOUNG

Head of Automotive
Partner, Gowling WLG

☎ +44 (0)20 3636 7968

+44 (0)7818 003 990

✉ stuart.young@gowlingwlg.com

SUMMARY OF KEY FINDINGS

Cyber-attacks targeting automotive systems and vehicles have hit the headlines during the last few years. In a future where CAVs are commonplace, hacks could threaten both the safety and privacy of all road-users. They have already had a major impact on car manufacturers, with millions of cars being recalled for vulnerabilities to be fixed, not to mention the effects of widespread, negative media coverage.

A recent instance occurred in the spring of this year when Hyundai had to patch its Blue Link smartphone app to stop it releasing private data that could, it was claimed, be used to break into and steal people's cars. Essentially the previous versions were transmitting personal information about registered users and their vehicles, including usernames, passwords, PINs, and GPS location records, back to Hyundai using HTTP encrypted with a fixed key. This key could be extracted from the application's code allowing a hacker to eavesdrop on the app's network connections, steal the data and decrypt it using the key.

This vulnerability in theory made it easy to find, unlock, and start a victim's car. They could essentially steal your keys. Hyundai fixed this before any problems occurred but it's a good warning of the potential problems.

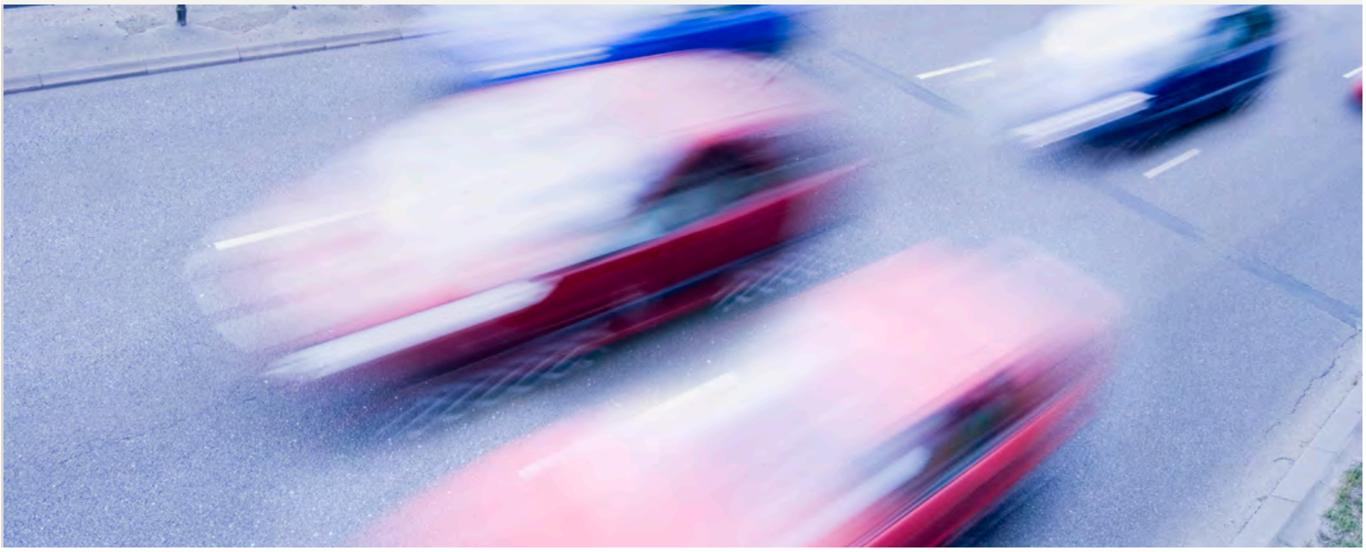
Our research has found that the motor industry is good at dealing with traditional car safety, but until recently was not necessarily accustomed to handling and mitigating cyber risks when developing CAVs. As our vehicles become increasingly sophisticated, and connectivity increases, thus introducing a growing number of touchpoints with the external environment and third parties, these risks will only increase.

— Stuart Young, Head of Automotive at Gowling WLG, highlights the pressures on the manufacturers:

> "Excessive regulation can have a deadening effect on any developing technology. However, responsible industry players usually welcome good regulation knowing that it provides a commercially level playing field and reduces the worry that there could be a "race for the bottom" where safety and security are sacrificed in the short-term interests of market share and profit. The automotive industry has a strong track record of improving safety in a collaborative way and that same spirit now needs to be applied to the development of CAV technology, especially in setting communications standards."

THE MAIN PROBLEMS IDENTIFIED BY OUR EXPERTS ARE:

- There is not enough collaboration among the manufacturers themselves. The desire to be first-to-market and create unique selling points (USPs) means discussions on best practice and setting standards are not moving as quickly as needed.
- CAVs are evolving from the less intelligent cars most of us drive today, but even these vehicles rely on software for many of their functions. CAV software is being developed out of old software and it is practically impossible to separate the old from the new. So errors and vulnerabilities will move into the new generation of CAVs.
- There is huge competition between the motor manufacturers, as well as from disruptive new entrants, to develop CAVs. This commercial pressure means those writing CAV software are potentially exposed to unrealistic deadlines when it comes to ensuring cyber resilience for their products. They need time to build systems and cyber security gateways adequate for vehicles with an estimated road life of 15 years.
- The existing testing regime which all new cars must go through, is not fit-for-purpose for CAVs.
- While the existing legal framework is broadly appropriate, our interviewees suggest some additional regulation would ensure CAVs were safe, and are perceived to be so by the buying public.



WHAT (AND WHERE) IS THE RISK?

The car on your drive is a result of years of development – power steering, aircon and even electric windows were once the preserve of the luxury market. Now we expect them as standard. These systems and the myriad others that make an "ordinary" car work, have been incrementally developed.

CAVs are the next stage in this development. But this evolutionary approach presents a major problem for auto manufacturers.

CONNECTIVITY RISKS

When motor manufacturers started adding automation to their vehicles, an Intelligent Parking Assist System for example, cyber security was not then recognised as the serious issue it is today. And our interviewees agree that it is the connectivity of CAVs that pushes cyber up the safety concerns list. There are risks associated with automation (which will be discussed later), but insecure network connections are one of the easiest access points for a hacker.

Professor Martyn Thomas CBE, Professor of IT at Gresham College puts it in context:

> "CAV manufacturers have a huge potential vulnerability. There are 100 million lines of software in a connected vehicle, never mind an autonomous one. And this software has not been written from the ground-up by the manufacturer or its suppliers. A great deal of it is legacy software. Some of it even comes from open source libraries on the internet, so there is huge potential vulnerability."

Perhaps the safest cyber solution is to proceed with automation and put connectivity on the back-burner? But as shown in the CAV communication types listed below, it is this connectivity that delivers many of the benefits:

- Tactical, short range communication, which is mainly vehicle-to-vehicle (V2V). For example, when a CAV "tells" another that it is about to pull out of a blind junction. This is a safety-critical system.
- Strategic communication, mostly longer range and involving vehicle-to-cloud (V2C). For example, when a driver receives notification of an accident on his route. There are obviously safety aspects to this too, but it usually focuses on long-term prevention or journey planning.
- Infotainment, including WiFi hotspots, weather information and music streaming. These are mostly focused on the convenience and comfort of the driver.

The recent SMMT position paper on connected and autonomous vehicles focuses on the importance of all CAVs being connected to the digital infrastructure. It says that:

> "ubiquitous coverage is the automotive industry's top priority."

In fact, vehicle connectivity will become part of the EU legal framework from April 2018, when all new vehicles will have to be fitted with a system called eCall. This sends an automatic message to the emergency services containing the location of a vehicle involved in an accident using an in-built GPS location device. So connectivity, and its associated cyber risk, will be part of everyday motoring from next year.

THE DEVELOPMENT OF CAVS IS CATEGORISED INTO SIX LEVELS ILLUSTRATED BELOW:

	Driver control	System control
Level 0 DRIVER ONLY	Driver is responsible for the vehicle. Controls lateral and longitudinal movement at all times.	System may provide alerts and warnings when driver fails to exercise control.
Level 1 DRIVER ASSISTANCE	Driver is responsible for the vehicle. Controls lateral and longitudinal movement at all times.	System can support lateral OR longitudinal control.
Level 2 ADVANCED DRIVER ASSISTANCE	Driver is responsible for the vehicle. Controls lateral and longitudinal movement. May hand some control over to the system. Must actively monitor system performance and retake full control where necessary.	System can control lateral OR longitudinal movement in specific use cases.
Level 3 ADVANCED DRIVER ASSISTANCE	Driver is responsible for the vehicle. Controls lateral and longitudinal movement. Can hand full control to the system. Must actively monitor system performance, retaking control as necessary.	System can control lateral AND longitudinal movement in specific use cases. Where system exceeds performance limits, it will hand control back to the driver.
Level 4 HIGHLY AUTOMATED	Driver is only responsible, and exercises control, outside of specific use cases where the car is able to self-drive.	System can control lateral AND longitudinal movement in specific use cases. It will not require driver intervention during this time.
Level 5 FULLY AUTOMATED		System can control lateral AND longitudinal movement in all use cases. Driver intervention is not needed.

It is interesting that the most readily-used technology shorthand focuses entirely on the autonomous elements and not on connectivity. The physical movement of vehicles seems to have a higher priority (or at least more accessible engagement) than the connected elements.

Until very recently, most people in the industry thought vehicles would develop through the stages. However, it now appears that most experts believe we will skip Level Three autonomy completely. This is because once autonomy takes over the driver "switches off" and needs time to metaphorically get back in the driving seat. For example, Ford found that during testing of its self-driving fleet, the humans in the car i.e. supervisors who were able to take control if necessary, lost "situational awareness" during the tests. According to Bloomberg, they had to use alarm bells and lights to keep them alert.

Stuart Young, Partner at Gowling WLG, adds:

"A study published in 2014 suggested that drivers take about 15 seconds to resume control and up to 40 seconds to stabilise vehicle control. That gap is much too long to offer any realistic prospect of human interaction preventing accidents."

Anna Bonne, Head of the Transport Sector at the Institution of Engineering and Technology (IET), echoes this:

"What we hear is that many of the car manufacturers simply aren't bothering with Level Three any more. It is just way too complicated – so they are concentrating on Level Four – the likelihood is that one of the German manufacturers will come out with an advanced autonomous vehicle soon."

This only adds to the pressure on manufacturers to enhance the cyber resilience of their CAVs sooner rather than later.

Peter Davies, Technical Director at Thales e-Security who provide expertise on infrastructure systems and cyber security to the UK Autodrive programme, agrees:

"The main problem for me is that we are looking at a bottom-up design from which we have to get safety-critical solutions. This is incredibly difficult for a hyper-connected system where all cars are connected to each other and there isn't a place to start from. Particularly as up until now, the process for safety critical systems has been to work out what the system is and work down."

Patrick Arben, Partner at Gowling WLG, draws a parallel from his experience with transport sector clients:

"Automotive is not the only sector facing the challenge of designing cyber security into an infrastructure which is already highly evolved. There may be learning points which can be borrowed from other safety critical industries such as aviation."

AUTOMATION RISKS

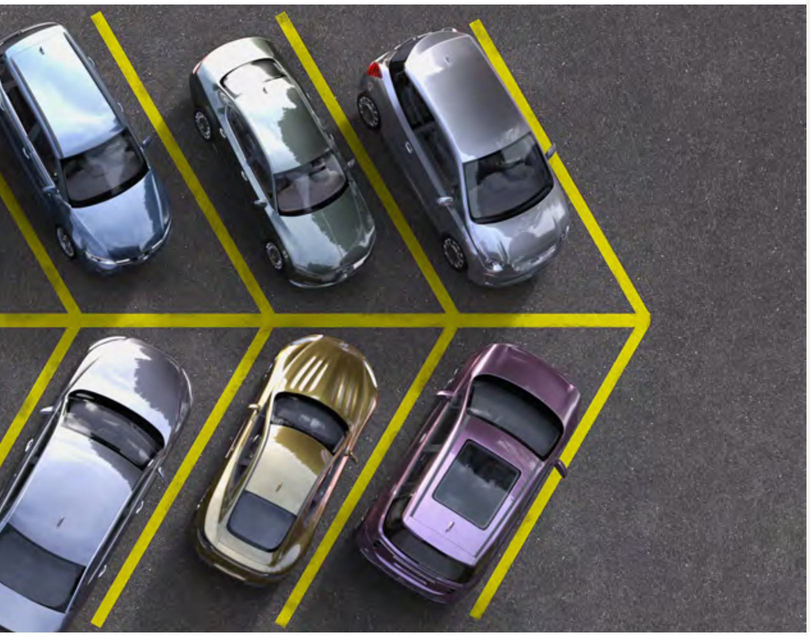
As mentioned earlier (on page 6) there are also cyber risks attached to the basic automated functions of these new vehicles.

Professor Thomas says that all the sensors in the vehicles are potential "attack vectors" – a hacker's entry point. Lidar is one of the sensor technologies that most autonomous vehicle manufacturers are including in their navigation packages and this can be attacked locally and spoofed and even GPS can be jammed.

He added:

"The data in the vehicle itself is a sensitive spot. So for example, someone could corrupt the mapping data or the data embedded in the machine learning system, leading to a very effective cyber-attack. This would probably affect all vehicles in a fleet and could lie undetected for a long time."

This sort of attack would take a great deal of planning and funding, and involve more than a teenager in his bedroom to perform it successfully. But the risk is there.



MORE COLLABORATION NEEDED

Motor manufacturers are intensely competitive. Each one wants to make sure that it is their vehicle that sits on your driveway.

Professor Phil Blythe, Professor of Intelligent Transport Systems at Newcastle University and Chief Scientific Adviser for the Department for Transport (DfT) says:

"The car companies will collaborate on standards where there is a need to open the market through interoperability, however in many cases they would prefer to act alone and define their USPs which make their product more attractive than their competitors."

And Stuart Young, Partner at Gowling WLG, agrees

"Vehicle manufacturers are generally concerned about this, not because they aren't keen to share the data but because they want to ensure the mechanism through which data is shared is sufficiently secure and will not compromise system integrity."

Recent examples of cyber-crime, particularly those involving Ransomware, have shown that hacking is a very real and immediate threat. Our experts believe that more industry co-operation would enhance CAV development and make them more cyber resilient.

Peter Edwards, Chief Architect and Cyber Security Lead at Arup – the lead partner for UK Autodrive and responsible for programme management and technical coordination – says:

"The industry is moving in the right direction by setting up consortia like UK Autodrive. But I think they all recognise there is a long way to go. Measures of success in cyber security are weak and there is a danger of attractive functionality being presented before all its ramifications have been thought through."

BUILDING RESILIENCE AND FUTURE-PROOFING

As consumers, we now expect our devices to "talk" to each other. This explosion in the number of connected devices has become known as the Internet of Things (IoT). CAVs are a further addition.

But each time something is added to this list, it increases the pressure on all organisations to increase their cyber resilience – and the pressure is showing.

According to the most recent edition of EY's Global Information Security Survey[2], 87% of the 1735 C-level executives they spoke to in global businesses, lack confidence in their organisations' level of cyber security.

[2] Path to cyber resilience: Sense, resist, react. EY's 19th Global Information Security Survey 2016-17.

So, what is the motor industry doing now, and what does it need to do more of, to minimise cyber risks and make sure every vehicle is resilient?

Encryption, layering, gateways and authentication are all part of current development activity. On top of this, manufacturers are using virtualisation or hypervisor solutions to separate safety critical functions from non-safety critical.

An industry member confirms:

> “It would be inconceivable these days for a manufacturer to bundle infotainment systems together with safety critical vehicle control systems or autonomous emergency braking. Infotainment, which is relatively more exposed to third party applications, could be the path in for a hacker.”

Peter Edwards at Arup confirms:

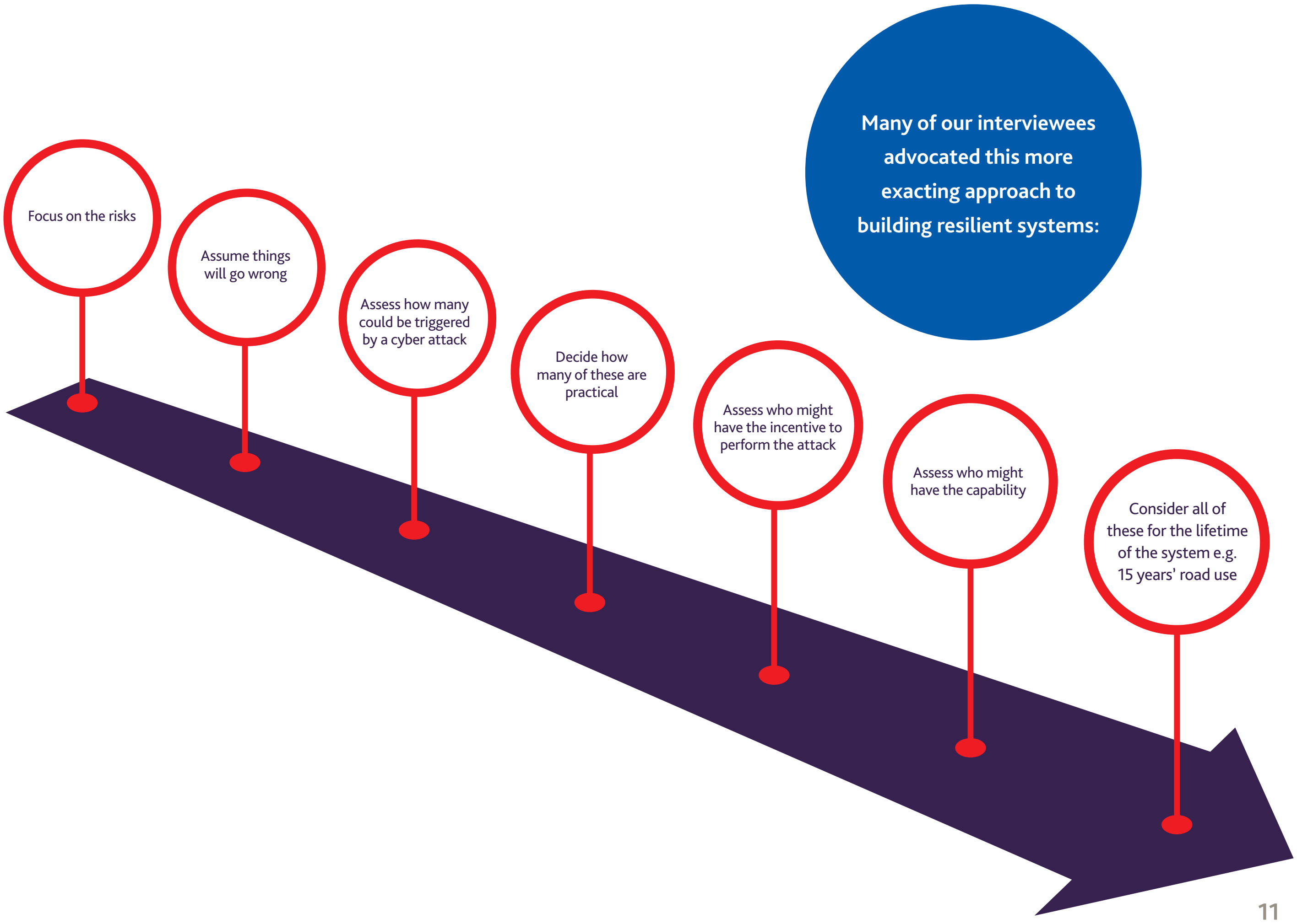
> “One example is that manufacturers are now splitting the infotainment system from the driving system. This is a blindingly obvious solution from a cyber point of view, but it does show that sensible engineering is now happening.”

CYBER SECURITY AS AN ENGINEERING DISCIPLINE

It is a “sensible” approach to cyber engineering that emerges as a key theme of our research.

Professor Thomas highlights this:

> “I want industry in general to wake up and realise that software development has got to become an engineering discipline. It can’t carry on as a ‘craft’, as it is now. This means we must routinely use mathematically rigorous specification, development and assurance methods which prove that software has the properties it ought to have.”



Many of our interviewees advocated this more exacting approach to building resilient systems:

- Focus on the risks
- Assume things will go wrong
- Assess how many could be triggered by a cyber attack
- Decide how many of these are practical
- Assess who might have the incentive to perform the attack
- Assess who might have the capability
- Consider all of these for the lifetime of the system e.g. 15 years' road use

Professor Blythe reiterated this:

> "We don't know every line of code that goes into each vehicle or why it's there. A typical German car has millions more lines of code than a jumbo jet. The latter was designed as a system all the way down and cars have tended not to be."

If the motor industry needs help to achieve this then our experts highlight two major sectors which could help – rail and aviation.

And Peter Davies adds:

> "There are also technologies coming out of robotics for example. The algorithms written for robotic systems that help them to learn can be used for CAVs."

Nadim Choudhary, an Associate at Arup, dealing with Resilience, Security and Risk believes:

> "You can never get risk down to zero. What we are talking about is reducing the residual risk, using principles described as 'as low as reasonably practicable', a principle which is well embedded and used within the Railways. Systematic embedding of cyber resilient elements into the technology we are developing is the way forward."

Modern air traffic control systems have used this approach, and according to our interviewees this approach was cost-effective for them. The aviation industry did considerable research and testing to work out how much it could trust GPS to land planes, for example. It took them a long time to understand the spectrum of vulnerabilities, but now they use the system to good effect while not opening it up to unacceptable risk.

So for CAVs, manufacturers need to understand what the vulnerabilities mean and then engineer alternative compensating controls that will be able to spot when a system has failed, in other words a multiply-redundant system.

TESTING

The vehicles we're driving now have all been put through their paces before they go on the road. This is known as penetration testing. Manufacturers currently employ 'ethical hackers' to do the Penetration Testing, to make sure their systems are immune to cyber-attack.

There are however problems with this approach, including:

- There is no mandated standard for penetration testing, and manufacturers select their own penetration testers.
- Guidelines exist, but they need to be changed to make sure they cater for the more sophisticated vehicles arriving on our roads.
- Penetration testing is a snapshot in time. It shows that one individual on a particular day cannot access the system.
- As highlighted earlier, CAVs use components that were built years ago in non-systematic ways and are therefore, packed with errors. The typical programmer makes between ten and 30 errors in each 1,000 lines of code, and it is recognised that a significant number of those are cyber security vulnerabilities. Testing only finds the ones that are easiest to encounter. A malicious hacker therefore, merely needs to try all the outlier cases.

Peter Davies commented:

> "I wouldn't expect anyone to test a plane a bit and then stick it in the air without being able to produce files of calculations that prove that the testing was successful. Using Penetration Testing to find how a potential hacker could hack is a fundamentally flawed way of going about it, because they will always find a way that we haven't!"

So what is the answer to this problem? Our experts suggest that there are two possible approaches, which, when combined, would greatly improve the cyber security of CAVs:

1. **Simulation** – used by other industries, including those in the transport sector.
2. **Regulation** – or a set of industry-formed guidelines.

SIMULATION

Technically, simulation is an accepted tool in engineering development. It is known to be a cheaper, safer and sometimes more ethical solution than conducting actual experiments. It is also a lot quicker, because simulations can often be conducted faster than real time.

Peter Edwards sums this up:

> "I believe a large part of the answer will lie in large-scale simulation and the associated analytics of the results. We could explore, very quickly, many of the avenues where things might go wrong and their consequences. For example, this could show us how non-critical vehicle systems interact and the potential failures they could propagate."

Professor Thomas highlights this problem:

> "We have to consider what happens when we update the software – do we have to test the vehicle all over again? If we do then that would make it completely unfeasible to ever update the software. If you change a line of code, then it is essentially a new vehicle, so logically you have to go through certification again."

As powerful as simulation is, it cannot be used on its own and would need to be combined with other real world testing. In addition, any updates designed by simulation would need to be regression tested to ensure that they did not inadvertently weaken existing systems and make them vulnerable to hackers.

REGULATION

The level of testing (simulated and real) would need to be agreed across the industry to ensure that acceptable security standards were met. How legally strict does that guidance need to be? We discuss setting the common standards for CAVs, and how this will be done in the next section.

GUIDELINES OR REGULATION?

It's clear that connected vehicles need to be built to common standards for interoperability, as well as safety reasons. But who sets those standards and how? In relation to the cybersecurity aspects of the standards, there are two approaches to ensuring the vehicles on our roads are cyber secure. Firstly, the manufacturers voluntarily agree to follow a set of guidelines, or alternatively they are compelled to do so by a new legal framework.

SETTING STANDARDS

Anna Bonne commented:

"The DfT wants to have a light touch on this – they don't want to hinder innovation. I think this is right, because we want to make the UK a leader in the CAV field. The UK needs to make money out of this, and with too much regulation this won't happen. I think we will only regulate if other countries do the same."

Peter Edwards also believes that setting standards is a better approach than regulation, but adds:

"I think there is a need to set better standards to which everybody in the industry can work, including measures of cyber resilience. There is a parallel with the construction industry – a few decades ago a few injuries and fatalities were just considered part-and-parcel of the sector. But now safety thinking has become engrained at all levels – from the Board down – to the point that there are hardly any deaths. We should concentrate on embedding cyber security thinking throughout an organisation."

Peter Davies agrees with this:

"The problem with existing standards and tools is that they aren't designed for a system of this scale or for one that is developing as quickly as this. So they are not directly applicable."

The majority viewpoint among our experts is that improved guidelines will be more appropriate and that increased regulation may stifle innovation. They also agree that the existing legal framework is strong enough because it is aimed at risk management. UK health and safety legislation encourages the identification of risk and the taking of reasonably practicable measures to ensure safety. This applies to product design and covers road safety. Breach is a criminal offence. The threat of criminal charges even for the creation of a risk should be enough to encourage compliance.

However, our panel suggests several areas where they felt new law may be helpful:

- Issuing updates
- Data sharing
- Penetration testing
- Accident investigation

ISSUING UPDATES

In the new Automated and Electric Vehicles Bill announced in the Queen's Speech in June this year, car owners will be made liable under their insurance for accidents if they have decided to modify the software on their vehicle or have failed to install important updates. Currently, however, there is nothing compelling manufacturers to issue those updates.

Peter Edwards comments:

"Perhaps this is an area where we need legislation. If a vulnerability is discovered in the software, then possibly legislation is the thing that forces that to be updated as soon as reasonably practicable. We have to build the facility into the vehicle to do regular updates and to make sure that these updates don't affect other parts of the system in a detrimental way. I think the obligation to make something safe and keep it safe to an agreed future date reflecting the vehicle life (15 years perhaps), could be written in law."

Legislation in this area for CAVs would make a WannaCry-type cyber-attack far less likely. This was a global ransomware attack targeting computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in Bitcoins. The attack began on Friday May 12 this year and within a day had infected more than 230,000 computers in over 150 countries. The NHS, Spain's Telefónica, FedEx and Deutsche Bahn were hit, along with many other countries and companies worldwide.

Since the attack we have learned that Microsoft produced a fix for the vulnerability exploited by WannaCry in February 2017. However, they only released it to their newer operating systems (OS). Any computers still using the XP OS were not updated because Microsoft stopped supporting XP in 2014.

Professor Thomas comments:

"It appears (from the dates that the Windows patches were cryptographically signed by Microsoft) that the XP fix was developed at the same time as the fix for the supported versions of Windows, although Microsoft only issued the XP fix once the scale of the attack became clear. The delay in patching XP might have been for commercial reasons, perhaps because Microsoft didn't want to give the impression that they were still supporting XP and therefore dissuade people from buying the newer versions, but the effect, regardless of commercial intention, was to leave customers such as the NHS vulnerable to attack and Microsoft subject to negative publicity."

DATA SHARING

The SMMT supports the manufacturers' view that guidelines are preferable to regulation. However, this does put them at odds with part of their membership – those from the after-market such as KwikFit and Halfords.

This argument centres around the use of the vehicle generated data e.g. speed, battery status and vehicle location. It does not concern data brought into the vehicle via your phone or anything that your roadside connections generate – conditions of the components and performance data for example.

Manufacturers are suggesting that access to this data will come from an off-board server which will be owned by the manufacturers. Third parties are welcome to access the data from this, but not directly over the air from the vehicle. Third parties are also welcome to set up their own server to draw data from the off-board server. So for example, IBM could set up its own neutral server to draw upon the data which it can then pass on to third parties who want to use it.

The manufacturers argue that if they allow unfettered over-the-air access to vehicle data in real time via an open interface when the vehicle is moving, the security of the data access, and by extension that of the vehicle, cannot be guaranteed. This, they claim, is akin to an open door for hackers to attempt to gain access to the vehicle's safety critical systems.

Bernardine Adkins, Partner, Head of EU, Trade and Competition at Gowling WLG, said:

"However, the after-market and independent garages argue this is anti-competitive, because the manufacturers can, if they wish, control what datasets they provide via their off-board servers and the messages that are served up to drivers on the in-vehicle interface. So for example, information about servicing, or predictive maintenance, can be shown to the driver with the subtle aim of encouraging them to send the vehicle to a franchised dealer or garage rather than an independent one."

At the moment, the manufacturers are trying to prove that they can provide all the information the third parties want, securely using a quality-assured process. So there won't, for example, be a lag in terms of transfer. The after-market, however, is very keen for Brussels to legislate, because they believe this is the only way they can guarantee they will get all the data. The debate on this continues at European Parliament level.

Again there are precedents to follow from other industries in this area. The DfT is currently working with the train operators to encourage them to share more of their data.

Anna Bonne told us:

"The DfT is having a positive response, although because of the franchise situation they can dictate to the train operating companies a bit more."

TESTING

Many of our interviewees believe that new legislation would be an effective way to improve the existing testing regime.

Nadim Choudhary comments:

"The threats are always changing, so we need to have a number of different responses, of which policy and regulation is one. In the railways, a train cannot go into operation before a safety case has been issued. This is written in law. So perhaps this should be required as part of the testing regime for CAVs also?"

Before the law is enhanced in this area, however, there's one key question that needs answering. If, for example, you have a regime that is reliant on testing as a way for a vehicle to show it is safe enough to go on the road, firstly you need to specify the criteria and conditions for the testing.

Professor Thomas adds:

"Are we looking for cars that are say, to a 50% confidence level, as safe as a human driver? If this is correct, and you want it to be true under all road, weather and lighting conditions for example, then we have got a hell of a lot of testing to go through. And somebody has got to be able to authenticate those results."

ACCIDENT INVESTIGATION

Another area highlighted by our experts concerns how accidents are investigated.

CAVs will carry their own equivalent of a black box. It is called the Data Storage System for Automatically Commanded Steering Function or DSSA and acts as an event data recorder for automated driving for Level Three cars and higher. It also logs limited data for a short period of time when automated driving mode is active, even if there is no accident. It is thought the data may be useful evidence to prove who was in control of the vehicle in the event of traffic violations.

The SMMT clearly states in its recent positioning paper that this must be regulated internationally.

Professor Thomas goes a little further on this area. He explains that all the data needs to be collected in a way that keeps the evidence-chain intact and collected in a format that can be independently assessed.

He said:

"I would really like to see legislation that allows for an independent after-the-fact investigation into the causes of an accident. The independent assessor needs to know where in the system the data was collected, so they can work out where it was collected, whether it could have been corrupted, and therefore whether the 'answers' are true. So if the system says the driver was braking, then is there a mapped system and data to back this up?"

He continues that it is critical that people other than those who are being sued are able to analyse that data.

"Otherwise there is a fundamental conflict of interest. The data that is recorded and how it is recorded really needs to be regulated."

The task for the regulators is to make sure that UK motor manufacturers and their supply chain colleagues benefit from improved legislation. Rather than become tangled in a patchwork of laws that merely add to their compliance challenges.

Helen Davenport at Gowling WLG comments:

"As an example, existing and forthcoming privacy legislation is also likely to be relevant in the area of data sharing and accident investigation."

CONCLUSION

CAVs should bring numerous benefits. But as part of the Internet of Things they need to be secure from cyber-attacks now and have an in-built resilience which means they are future-proofed.

SETTING STANDARDS

In particular we recommend that:

- Manufacturers must use a recognised process for developing the cyber security of their CAVs. This must include the necessary design and testing phases, as well as a process for updating systems 'in the field'.
- The system of testing needs to be looked at in-depth. Regulation of this area should be considered in order to ensure a consistent approach and public confidence.
- Regulation should also be considered to ensure software updates are issued in a timely manner and 'black box' recording systems are storing the right data in an incorruptible way.
- The motor industry must not under-estimate the threat. They must act more collaboratively, share information and adopt best practice procedures that have been developed by the industry, for the industry.

Professor Blythe comments:

> "You can't take a jumbo jet and hide it in a hangar for months and try to crack its codes – but with a car you can. So I think the risk is high. I don't think the benefit of doing the hack to vehicles is there at the moment, but once there are more automated vehicles and they are all connected to the infrastructure then a denial of service could be a really significant challenge."

Cyber time advances faster than the hands of your watch. People sit and think about decisions, cyber threats don't. Manufacturers need to act now to ensure their CAVs are secure.

GOWLING WLG (UK) LLP
T +44 (0)370 903 1000
gowlingwlg.com

GOWLING WLG

Gowling WLG is an international law firm comprising the members of Gowling WLG International Limited, an English Company Limited by Guarantee, and their respective affiliates. Each member and affiliate is an autonomous and independent entity. Gowling WLG International Limited promotes, facilitates and co-ordinates the activities of its members but does not itself provide services to clients. Our structure is explained in more detail at www.gowlingwlg.com/legal