CONNECTED AND AUTONOMOUS VEHICLE

WHAT ARE THE RISKS AND THE WAY FORWARD

CYBER SECURITY

According to an independent study by KPMG for the Society of Motor Manufacturers and Traders (SMMT) on March 2015 (http://www.smmt.co.uk/wp-content/uploads/sites/2/CRT036586F-Connected-and-Autonomous-Vehicles-%E2%80%93-The-UK-Economic-Opportu...1.pdf) , the Connected and Autonomous Vehicle (CAV) sector in the UK will provide an economic and social benefit in the region of £51 billion per year by 2030.

The Department for Business, Innovation and Skills (BIS) has shown its interest in promoting research and capture the value of the Connected and Autonomous Vehicle (CAV) industry through joint initiatives with the Department for Transportation crating the Centre for Connected and Autonomous Vehicles (C-CAV) among others. BIS is also partnering with other governmental entities to achieve such goal.

There is no doubt that the fast adoption of CAV technologies in the automotive sector is clearly a great opportunity for growth. The UK automotive manufacturers as well as the public authorities must be swift in embracing the development of new technologies and provide a safe and secure framework for this type of cars, from cyber security to regulations.

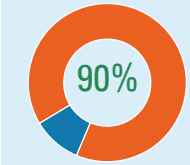
But with opportunity also the door to news risks is open. There already are public instances of CAV components being 'hacked' so an attacker could manipulate vital car functions, such as the breaking assistant or controlling remotely the car's engine.

This race for CAV technologies adoption implies for manufacturers to include the 'secure by design' concept in the development of their devices. It also calls for the secure management and processing of data and information, personal and mechanical mainly in:

1. Decision making software
2. Vehicle Cyber Security
3. Data opportunities

CONCERNS

Internet of Things (IoT) is a new market with an **immature security culture**



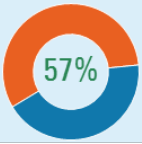
THINK THT IT IS DIFFICULT to secure automotive applications

- Devices are built with new protocols that often use **insecure means of communication**
- There is an absence of standards at this point
- There are **too many vendors** in the IoT space, each building to their own specifications
- Software **security state is similar to how software security was in the 90s** – for firmware, BOTH mobile and backend
- **Security implementation is weak** due to low power/ incentives and potential cost – the age old debate of potential **ROI**

WHAT'S AT RISK?

The inclusion of telematics and Internet of Things devices in the insurance and automotive sectors and the speed of adoption of these technologies open new risks for:

- **Data Privacy:** Unauthorised disclosure of information could be caused by issuing commands to the devices in a private or corporate environment to transmit personal or confidential information to the attackers.
- **Customers safety:** As CAVs rely more in the automated functions, the compromise of the devices that make those functions possible could cause material and human damage. There have been recent events of hackers taking control of vehicles (Jeep Cherokee) resulting in the recall of 1.4 millions units.



DOUBT THAT AUTOMOTIVE software development team have the skills necessary to combat software security threats

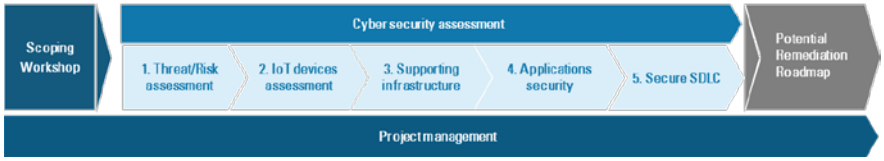
> It is estimated the UK could obtain social and economic benefits of over £51 billion a year by 2030 and be part of an estimated market of £900 billion worldwide by 2025.

WHAT'S ON YOUR MIND?

- Is my supplier of telematics devices including Secure by Design methodologies in their Systems Development Lifecycle process?
- Are the applications used by your customers to send over personal information resilient to data leakage?
- Are your customers safe from an attack that could cause their cars to be compromised when on the road?
- Is my Data Analytics provider correctly managing your customers personal information and giving you a meaningful view/interpretation of their driving patterns?

IS THERE HELP TO UNDERSTAND AND PROVIDE ASSURANCE?

Our proposed approach is tailored to meet requirements. The approach comprises of one work stream with phases that will enable us to focus on specific and inter-related areas. This phased approach enables us to be flexible in the type of work we perform and the timing of the work.



HOW WE HAVE HELPED OTHERS

KPMG Approach

A through and comprehensive security review which was broken down into four work streams:

- Hardware testing of the telematics devices families;
- Security testing of software ranging from Device Firmware to business mobile and web applications;
- Testing of the entities security posture and;
- An architecture review of the data centre and security operations.

Value

Through working on this engagement we were able to apply our telecommunications and Machine to Machine (M2M) networks expertise to assess the security of our client's infrastructure and products. This further expanded our own knowledge and understanding of automotive and telematics security.

The security assessment highlighted numerous major and previously unknown vulnerabilities in the Telematics devices and applications as well as significant threats to the telecommunication organisation itself. All this information was provided in time to enable the Client to take an informed strategic branding decision.

POTENTIAL BENEFITS TO YOU

- An independent and objective assessment of the security of the telematics and connected devices deployed to your customer base and vehicles.
- A clear statement of the security risks and priorities to allow you to focus on fixing the most important issues.
- The identification of the critical assets, threat landscape and risk controls over threat events effectivity in your organization and sector.
- Assurance provided to Boards that IT Security is being managed appropriately.

Produced by Create Graphics

www.kpmg.com/uk/cyber #feelfree

WE BELIEVE CYBER SECURITY SHOULD BE ABOUT WHAT YOU CAN DO – NOT WHAT YOU CAN'T

WHY KPMG?

INDEPENDENT

Our technical strategies and recommendations are based solely on what is fit and appropriate for your business.

COLLABORATIVE

KPMG's I-4 forum brings together over 50 of the world's leading organisations to discuss emerging issues and the solutions which work in an ever-increasing threat landscape.

TRUSTED

KPMG member firms have a long list of certifications and permits to work on engagements for the world's leading organisations.

GLOBAL, LOCAL

KPMG is a global network of independent member firms of over 162,000 professionals in 155 countries.

We have over 2,000 security practitioners globally, giving member firms the ability to orchestrate and deliver a high level of quality worldwide.

Contact us:

John Leech
Partner, UK Automotive
T: + 44 (0)21 232 3035
E: john.leech@kpmg.co.uk

Jim Fox
Director, Cyber Security
T: + 44 (0)20 7694 5100
E: jim.fox@kpmg.co.uk

Rick Marriott
Executive Advisor, Cyber Security
T: + 44 (0)20 7311 6026
E: richard.marriott@kpmg.co.uk