QUESTIONNAIRE FOR AIDA WORLD CONGRESS, RIO, 2018

DRAFT/ ENGLAND AND WALES RESPONSE, prepared by Clyde & Co (Nigel Brook, Helen Bourne, Mark Hemsted)

New Technologies
(Autonomous Vehicles and Robots- Cyber Risks- New Technologies and Insurance Process)

General Co-Reporters: Kyriaki NOUSSIA and Rob MERKIN

I. DRIVERLESS/AUTONOMOUS VEHICLES AND VESSELS

1. **Are there any specific laws already adopted in your jurisdiction, or proposals for laws, relating to liability in tort for injuries inflicted by the use of such vehicles or vessels? If so, please provide a short explanation.**

Comment: answers may include the liability of drivers, producers of vehicles and the suppliers of satellite technology.

The Automated and Electric Vehicles Bill is the UK's current proposal for regulating autonomous vehicles. The purpose of the Bill is to allow innovation to flourish and to ensure the next wave of automated technology is invented, designed and operated safely in the UK. It is intended that driverless vehicles will operate on UK roads by 2021.

Insurers have been closely involved in the development of the Bill, which maintains the current insurance and regulatory regimes and will guarantee that nobody will be treated differently by insurers if they choose to 'drive' an automated vehicle.

The Bill was published on 18 October 2017 and is presently proceeding through the House of Commons. It will extend compulsory motor vehicle insurance, enshrined in the Road Traffic Act 1988, to cover the use of automated vehicles, to ensure compensation claims for injuries are paid quickly, fairly, and easily, in line with longstanding insurance practice and in compliance with the EU Motor Insurance Directive.

The Government recognises there are specific issues with regard to product liability in a motor insurance context. However it is not presently considered proportionate to make any changes to product liability law to facilitate the arrival of what will initially be a small number of autonomous vehicles in proportion to the whole vehicle fleet.

The Bill places liability for accidents involving autonomous vehicles on the motor insurer, with the possibility of subrogating from the manufacturer where the automated vehicle is at fault for the accident.

The proposed single insurance policy model is considered to be the most effective way to support a functioning market for automated vehicles, which ensures that innocent victims of an automated vehicle collision receive compensation quickly, fairly and easily, whilst allowing flexibility for the insurance industry to decide which insurance products they wish to offer.

The Automated and Electric Vehicles Bill mirrors the previous Vehicle Technology and Aviation Bill which was abandoned when Parliament was dissolved for the General Election in May 2017. Both Bills are product of several Government Consultations.

"Automated vehicles" are to be defined in the Bill by reference to a definitive list of vehicles, which is to be set and administered by the Secretary of State. The proposals make it clear that automated vehicles are only those that are capable of "operating in a mode in which it is not being controlled, and does not need to be monitored, by an individual". This equates to levels 4 and 5 of the SAE International's J3016 standard (also known as: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems).

The Bill retains the single insurer approach, contained in the Road Traffic Act 1988, whereby the injured party (including the automated vehicle 'driver') would be able to claim compensation from the insurer of the automated vehicle. In turn, the insurer will have a right of recovery from vehicle and software manufacturers (depending who was at fault / contributed to the accident).

Where the manufacturer is found to be liable, the insurer will be able to recover against the manufacturer under existing common law and product liability laws. The Bill provides two exemptions to the single insurer policy.

An insurance policy may exclude or limit an insurer's liability for damage suffered by an insured person arising from an accident occurring as a direct result of:

1. Alterations to the vehicle's operating system made by the insured person, or with the insured person's knowledge, that are prohibited under the policy.

2. A failure to install software updates to the vehicle's operating system that the insured person is required under the policy to install or to have installed.

This second exemption places considerable onus on the user to maintain their vehicle and as such manufacturers will need to make this process as easy as possible. It is possible that subrogation cases on these issues will go to court, although over time insurers and manufacturers will likely develop processes to handle most recovery claims quickly and easily.

In addition, insurers and vehicle owners will not be liable if the automated vehicle user was negligent in allowing the vehicle to drive itself when it was not appropriate to do so. This raises questions of what standards should be expected of someone 'driving' an autonomous vehicle and the marketing of such vehicles to consumers. Satellite litigation on what is to be considered 'negligent' is expected. The distinction between 'assisted' and 'automated' driving is significant for insures in this context and is further considered in Questions 3 and 4 below.

Existing product liability claims

As a matter of public policy, the Government has focused on current motor insurers as the first port of call for all third-party claims arising from an automated vehicle, in order to simplify the claims process.

The Government has resisted calls to update existing product liability law to account for the introduction of driverless cars to UK roads. However it is noted that a rolling programme of reform for driverless vehicle regulation is underway, so this should not be discounted in the future. The

approach is also inherently agile, allowing the next wave of reform to be commenced earlier if technological or other developments dictate.

The proposed reforms will not preclude proceedings being brought based on existing product liability legislation and the common law. In England and Wales, a claimant is able to bring an action directly against the manufacturer under the Consumer Protection Act 1987. Additionally, where the manufacturer is found to be liable, the motor insurer will also be able to recover against the manufacturer under existing common law and product liability laws, irrespective of whether the Bill becomes law.

Highway Code

The Highway Code provides essential information to all road users, summarising key road traffic law and providing further guidance about desirable and appropriate behaviours for drivers and other road users. Although the Code doesn't impose particular liabilities on road users for injuries in tort, it provides a framework of best practice for drivers, whose breach of the rules may be regarded as indicative of fault in the event of an accident.

The Government has noted it is important that, as well as reflecting legislative changes, the guidance in the Code reflects any implications of new technologies for drivers, their behaviour and other road users.

The Government proposes updating the Highway Code to explain ADAS motorway assist and remote control parking, and how they are to be used appropriately. It is important drivers use these systems responsibly, and that they do not attempt to use assist technology beyond what it is designed for, so that they can contribute to improving road safety.

When more advanced automated systems are approved and available, which allow the driver to be 'out-of-the-loop' and divert their attention away from driving and actively monitoring for parts of the journey, the Highway Code will be further amended to expand on this and provide fuller advice for drivers of automated cars and other road users. One example will be permitting a 'hands off' approach to driving as the technology develops.

Road Vehicle (Construction and Use) Regulations (as amended) 1986

The main domestic regulations affecting the design and operation of near to market technologies, such as remote control parking and motorway assist, are the Road Vehicle (Construction and Use) Regulations.

The Government has advised they are not aware of any regulation prohibiting the use of motorway assist systems as they are designed as a driver assistance function with the driver remaining in-the-loop throughout.

As autonomous vehicles become available and enable drivers to safely be out-of-the-loop for parts of the journey, the Government will reconsider these regulations. The Government plans to ensure that regulations do not unduly restrict activities the driver may safely engage in when out-of-the-loop.

As an example, Regulation 104 requires that a driver must always be in a position to have full control of the vehicle and full view of the road and traffic ahead. The Government proposes to clarify this regulation by adding a statement that a driver meets this requirement even if he is not in the driving

seat, as long as he has the ability to control the vehicle through a hand-held device. This amendment would cater both for remote parking via a hand held device, as well as very large vehicles or mobile transporters that are operated by remote control to aid manoeuvrability. Further revisions will be necessary as the technology develops.

The testing and regulatory environment in the UK is favourable compared to Europe and the US. The UK is likely to benefit from not being a signatory to the UN Convention on Road Traffic, which requires that a driver must be in the front seat of a car. This gives the UK a competitive advantage as it is flexible to set its own rules for testing which should allow innovation to flourish more quickly.

Autonomous vessels

The regulation of autonomous vessels is in its infancy in the UK. Amendments to the laws regarding the imposition of liability in tort for injuries are expected to follow those of driverless vehicles. The insurance industry will play a key role in enabling this; adapting existing insurance requirements is likely to be the biggest obstacle to the wider adoption of such vessels.

The Solent Local Enterprise Partnership (LEP) has awarded BAE Systems a grant to design and deliver the UK's first dedicated autonomous systems testing service. The new service will be ready for use later in 2017 and customers will be able to conduct trials and test systems such as unmanned boats, air vehicles and autonomous sensors in a safe, controlled and realistic environment in the Solent. Backed by a comprehensive safety case, the service will make use of a secure maritime communications network and a mobile command and control centre, featuring the same technology BAE Systems provides to UK Royal Navy platforms.

UK Minister Matthew Hancock officially opened a research centre dedicated to autonomous unmanned vessel activities. Based in Portsmouth the Centre for Maritime Intelligence Systems (CMIS) will set up an initial synthetic environment and conduct initial de-risking and "proof of concept" activities as part of a maritime autonomous systems demonstrator programme for both boats, submarines and 'other vessels'.

A central issue is where liability will fall, particularly delineating between the negligence of master, officers and crew. These risks are commonly covered as peril under British marine hull clauses, provided such negligence has not resulted from a lack of due diligence by the assured, owners or managers.

Determining whether a ‘captain’ sitting at a desk in port would be legally part of a ‘crew’ is likely to be viewed differently by various legal jurisdictions, as they apply the law to insurance claims for physical loss or damage to the ship. Regulations in respect of these issues will be required.

It will be important for the insurance industry to create a framework, similar to that created in the development of driverless cars on the roads, to determine who is liable in the event of an accident.

Within shipping, regulation is geared towards the safety of the crew, vessel and cargo, which all interact with one another. A vessel must be safe to ensure the safety of the crew and cargo; the cargo must be safe to ensure the safety of the crew and vessel; and for the vessel and cargo to be safe, there must be sufficient crew on board. Regulations will therefore have to react to the new type of crewless vessel.

Space Industry Bill

The Bill was introduced in the House of Lords on 27 June 2017 and is presently proceeding through the House of Commons. The Bill will provide a regulatory framework to cover operational insurance, indemnity and liability for commercial spaceflight and satellite use.

The Bill will:

- Create new powers to license a wide range of new commercial spaceflight, including vertically-launched rockets, spaceplanes, satellite operation, spaceports and other technologies.

- Create a regulatory framework to manage risk, ensuring that commercial spaceflight in the UK remains safe.

- Promote public safety by providing a regulatory framework to cover operational insurance, indemnity and liability.

These new legal duties will take on increased significance in the autonomous vehicles arena as automation and vehicle connectivity levels develop. The Bill provides for the strict liability of an operator for injury or damage caused in the United Kingdom or its territorial waters; to an aircraft in flight above such land or water; or to persons or property on board such aircraft.

The injury or damage must be caused by a craft or space object being used by the operator for spaceflight activities; by anything falling from such a craft or object, or by any person in the craft. This means that damages can be recovered without proof of negligence or intention or other cause of action.

2. Are there any specific laws already adopted in your jurisdiction, or proposals for laws, relating to compulsory insurance coverage for injuries inflicted by the use of such vehicles or vessels? If so, please provide a short explanation.

Comment: answers may relate to motor vehicle insurance and product liability insurance.

As identified above, the Automated and Electric Vehicles Bill will supplement the compulsory motor insurance regime (Part VI of the Road Traffic Act 1988) to include the use of autonomous vehicles, and establish a single insurer model, where an insurer covers both the driver's use of the vehicle and the autonomous vehicle technology.

This single insurer model would ensure that the driver is covered both when they are driving, and when they have activated the automated driving function. In the event of a collision while the automated driving function was active, the innocent victim (both inside and/or outside the vehicle) would be able to claim from the vehicle insurer.

The Government previously suggested extending the existing product liability insurance model to cover manufacturers of driverless cars, requiring drivers to purchase a separate product liability policy.

However, the Association of British Insurers opposed these proposals and noted a separate product liability policy "would be too complicated, risk leaving road accident victims without enough cover" and create a number of challenges:

1. Product liability insurance is currently optional, in contrast to motor insurance which is compulsory in the UK.

2. Cover for personal injuries under motor insurance is unlimited, whereas product liability cover may have limits, for example, £5 million or £10 million. This may lead to the level of recovery being determined by the type of insurance rather than by the severity of losses the injured person sustained.

3. There is a limitation on product liability claims of 10 years. Limiting claims according to the age of the vehicle would not serve the intended outcome of the Road Traffic Act, especially as motorists are under an obligation regarding the ongoing roadworthiness of their vehicles, whatever their age.

However, it is likely this position will need to be kept under close review and adapted as and when the UK motor fleet moves from mixed to largely autonomous vehicles.

Potential changes to the EU motor directive (currently in consultation) in respect of when compulsory motor insurance will apply to vehicle use will also have an impact in the driverless contact. If vehicle use is extended to use on private land, following the interpretation by the European Court of Justice in Vnuk, this is likely to lead to an unworkable compulsory insurance regime in the UK, where fraud is likely to run rampant. In addition there is likely to be difficulties in ensuring compliance and insurers will struggle to price premiums without reliable past data to assess the risk.

3. How do you envisage the future of personal lines in motor vehicle insurance in the next 5-10 years in your jurisdiction?

Comment: you may wish to comment on the future of motor vehicle insurance and the plans being made by the industry for new products

The future of personal lines in motor vehicle insurance in the UK will be dependent on the pace of change in the journey from assisted to fully autonomous driving.

The Association of British Insurers' most recent report, providing a UK insurer view of regulating automated driving (July 2017), notes that UK insurers, including AXA, Admiral, Ageas, Allianz, Aviva, Co-operative Insurance, Covea, Direct Line Group, esure, LV, RSA, Zurich and the Lloyd's Market, strongly support vehicle automation in the firm belief that it will deliver a significant reduction in the number and severity of accidents.

A key distinction is made between 'assisted' driving (employing automated driver assistance systems) and fully autonomous vehicles. Assisted driving exists at Levels 1-3 of the scale of autonomy, with Levels 4 and 5 representing fully autonomy. It is anticipated that in the next 5 years, only level 1-3 will be reached in vehicles on UK roads; with level 4 and 5 (currently prohibited in the

UK) to follow in the consumer sector from around 2025.

The Government's legislative plans will retain the insurance status quo in requiring the driver to incept insurance and for the insurer to pay claims even when operating in autonomous mode (with appropriate subrogated rights of recovery from the manufacturer / software provider).

In the short-term therefore the UK motor insurance market is likely to continue to operate in much the same way as currently, albeit with new right of recovery for insurers against liable manufacturers and software providers. This is likely to increase the costs of claims, particularly in the short term, until streamlined recovery channels are established with manufacturers and software providers.

In the longer term, the implementation of autonomous driving may largely depend on the willingness of the insurance industry to insure the risk. Insurers will be required to make fundamental changes to their rating and underwriting models and to their technology infrastructures. This will necessitate harnessing data from autonomous vehicles in order to fully assess the risks.

The increased adoption of telematics is regarded as one of the major turning points to the success of driverless cars. The penetration of telematics will increase in the next few years due to the development of cheaper after-market data produced by retro-fitted devices, as well as mobile phone applications. This will enhance insurers' understanding and use of advanced driver systems data and enable risk to be priced more accurately.

Telematics analysis will allow insurers to understand how and when a safety feature such as autonomous emergency braking is activated, how it influences driving behaviour and how that change will affect their pricing and their loss ratios. This will assist insurers to better understand how the technology is advancing from a safety perspective, so they can adjust their pricing accordingly. It will also allow vehicle manufacturers to invest in effective vehicle safety features.

Over the next few decades insurers will operate in a hybrid market space where there will be many different vehicles with different capabilities. The insights gained from the experience of these developing safety features can be applied to fully autonomous driving situations. For insurers, that most likely means monitoring the shift from personal liability to product liability.

Access to data will be key to understanding and pricing risk and may result in manufacturers, convinced about the safety features on their cars, insuring the vehicles themselves to reduce the cost of insurance for their customers. Google, Mercedes, and Volvo have all already announced they will be self-insuring their own products. Indeed self-insurance could be a good interim measure while insurers sort out their business model as the technology develops. However there is need for independent insurers to be involved as neutral arbiters of risk, letting technology developers focus on manufacturing vehicles and software.

The challenging nature of the motor insurance market may operate as a deterrent for manufacturers entering the insurance space. In addition to profitability concerns, current capital adequacy requirements mean manufacturers will need to capitalise to become an insurer. It is likely approximately 30% of the premium they collect will be held in reserve in the event of accidents, which many manufacturers will unable / unwilling to achieve.

An alternative model already seeing traction is partnership between insurers and manufacturers. Allianz has already partnered with BMW and Aviva is reportedly in talks with major manufacturers. Both deals would see drivers automatically receive insurance when buying a driverless car.

The claims process is also likely to alter dramatically. The Government has suggested an insurer will be able to seek reimbursement from the at-fault manufacturer. Without access to vehicles' data, insurers are in a vulnerable position in terms of proving who was at fault, whether it was the driver, installer, the retailer, the original manufacturer.

Collaboration or data sharing agreements will be required to ensure there is the appropriate information transfer. Insurers will have a significant role in assisting the development of sound risk management practices for autonomous and unmanned vehicles so it is considered such arrangements will be desirable in the market.

In a KPMG's 2015 survey, 45% of insurance executives indicated that as driverless vehicle use develops they expect to reduce premiums for motor insurance. Insurers have the expertise in pricing risk and manufacturers have the data for the vehicles to allow risk to be priced accurately. It likely that collaboration will be pivotal, providing data access issues are ironed out. Insurers may therefore begin to insure fleets rather than individual vehicles through agreements with manufacturers.

As automation develops, instead of today's car ownership model, we are more likely to rely on mobility as a service. Consumers will buy a service much like using an Uber. Pay per use policies from insurers in collaboration with manufacturers may become a new model. Thus, one alternative business model in insurance could be to charge for these micro-risks, and even with micro-payments of pennies per hour (or smaller increments of time) or per mile. There is concern traditional insurers could be pushed out of the market if they fall behind the trend.

However, in the transition towards driverless vehicles, insurers will need to be mindful of the potential for large unexpected losses which are hard to anticipate and cannot necessarily be mitigated by pooling risks over a large number of policies (and investing the resultant premiums).

This will be particularly stark if insurers are to insure fleets of new driverless vehicles in collaboration with manufacturers. Improved autonomy will change the nature of the insured risks and may mean that overall aggregate loss outcomes may become less predictable and highly variable. Indeed insurers would be subject to large scale aggregation risk as a result of a systemic failure affecting multiple vehicles. Additional reinsurance activity may therefore begin to be seen in the motor market.

Specific insurance policies are also likely to be brought to market. Adrian Flux has already launched its first driverless car policy which he said was, the first of its kind in the UK. The policy is designed for consumers who already have driverless features in their cars and will be updated as both the liability position and driverless technology evolves.

The driverless policy has additional features to a standard motor policy. It covers loss or damage in case of:

- Failure to install vehicle software updates and security patches, (subject to an increased policy excess);

- Satellite failure or outages affecting navigation systems, or failure of the manufacturer’s vehicle operating system or other authorised software;

- Loss or damage caused by a failure to manually override the system to prevent an accident should the system fail; and

- Loss or damage if the car gets hacked.

4. Driverless cars and autonomous vehicles apart, how do you assess the following technological developments that are expected to not only reshape the auto sector but also the insurance industry around it?

Comment: answers may include identifying the legal and regulatory regime and provisions in your jurisdiction.

(a) connected cars (i.e., Internet enabled vehicles, (IEV));

Vehicles in the UK are becoming increasingly connected; with the technology expected to become standard by 2020. Connected technology improves drivers' experience, their safety and increases efficiency. This is achieved by communicating information about the car and the driver to many sources. This can include insurance providers, breakdown services and dealership parts departments.

Connectivity will soon be a requirement. The EU has mandated that from April 2018 all new cars sold in the EU must have the capability to make an automated call to the emergency services in the case of an accident. Emergency contact centres across the EU were required to demonstrate their ability to handle an eCall from 1 October 2017, which can be either manual (vocal) or automatic (data via modem). In the UK, the infrastructure for dealing with eCalls has already been put in place by telecommunications technology company Avaya in preparation for the new regime.

The rise of connectivity raises important issues in respect of determining liability, data access and sharing and cyber security, which are only beginning to be addressed by regulators and industry.

Usage based insurance

Despite recent breakthroughs and indications of increased use of telematics or usage-based insurance (UBI) policies, the speed and scale of the impact of vehicle connectivity on the insurance market remains uncertain.

Delays in adapting business models may leave insurers vulnerable to competition from new entrants from adjacent industries and especially software led companies with specialisms in big data processing and analytics.

Perhaps the biggest current opportunity for insurers related to car connectivity is usage-based insurance (UBI). Products based on how often, where and how people drive enable insurers to price the risks more accurately, which can result in lower premiums for the insured taking less risk. The demand for insurance policies based on vehicle-based telematics has been growing and we expect the variety of policies available to increase in accordance with demand.

The opportunity for insurers also extends beyond the vehicle. By combining vehicle data with information from other sources, such as smartphones or public transit systems, an insurer could build a more complete picture of a driver's usage of mobility services irrespective of the type of transportation they use. This paves the way for insurers to develop new types of policies that insure a user for their broader mobility and not just driving. Already insurers are beginning to offer flight delay insurance utilising blockchain technology, which compensates insureds automatically if their

flight is delayed for more than two hours. Further parametric based usage policies covering other travel sectors are also likely.

As more vehicles are connected, there are more opportunities for insurers and automakers to analyse individual driving behaviour in the context of other drivers and other data, particularly in near real-time. Car connectivity enables insurers to establish regular touch points with drivers by using vehicle behaviour analytics as an early warning alert system that can also better predict new risks.

An insurer could potentially issue targeted notifications directly to a customer's dashboard to advise them, for example, that they should change to winter tires a little earlier than usual due to an anticipated cold snap. In the future this will allow insurers to proactively (and automatically) manage and simultaneous mitigate individual policyholders risks, creating a new business model for the pricing of motor risk.

Claims

Connected vehicles will be able to communicate with each other and record and store personal data, such as the number of passengers inside the vehicle. This information might include crash data, health conditions, biometric information and intellectual property, creating a complex picture for data regulators.

The Government recognises the importance of a data sharing framework to underpin the proposed changes to the compulsory framework for motor insurance, as data will be required to determine who was in control of the vehicle at the time of the incident. However, as data generated will likely constitute "personal data" for the purposes of the Data Protection Act and General Data Protection Regulation (GDPR) and will be necessary to address key liability issues in all driverless vehicles, it is likely international regulation will be needed.

The Association of British Insurers wants vehicles to collect a basic set of core data which would be made available after an accident. The data would cover a period 30 seconds before and 15 seconds after any incident. It would include the exact location of the vehicle, whether it was in autonomous mode or under the control of the driver, and whether the motorist was in the driver's seat and had a seatbelt on.

Data will clearly be required to determine whether the driver or the vehicle was responsible for any collision, such as establishing who was in control at the time of the incident. This is likely to come from in-vehicle data recorders. Many vehicles already have data recorders fitted, although the data collected is not accessible without special equipment. Liability disputes in the claims process may become a thing of the past, as connected vehicles become the 'perfect witnesses' to every collision.

We expect that the out-of-the-loop motorway driving vehicles that are coming to market soon will have an event data recorder fitted. There are inevitably different views as to what data is essential and of course data protection and privacy considerations are important. It seems likely that data recorders will need to be regulated on an international basis, like most vehicle technologies. The Government has pledged to participate fully in this debate, equipped with views from the UK manufacturing and insurance industries, evidence from the various trials taking place and the first connected technologies that are coming to market.

General Data Protection Regulation (GDPR)

UK data protection law will change on 25 May 2018 when the General Data Protection Regulation (GDPR) takes effect. The Government has confirmed that the GDPR will apply in the UK irrespective of Brexit and a recently published a statement of intent the government has proposed a new Data Protection Bill which implements the GDPR in full with a couple of amendments to ensure that the legislation works once the UK is out of the EU.

As with the DPA, the GDPR places obligations upon those who deal with data and it confers broad rights upon those whose data is processed. The GDPR includes a number of wide-ranging changes to EU data protection law, including:

- Tougher fines: Businesses will be subject to fines of up to €20 million or 4% of annual global turnover, whichever is higher, for infringements with some of the rules. These include infringements to basic principles for processing such as consent.

- 72-hour data breach notifications: A data controller must notify the relevant supervisory authority of a personal data security breach within 72 hours of becoming aware of the breach. They may also be required to inform the affected individuals where there is a high risk to their personal data.

- Accountability and privacy-by-design: Businesses will be required to demonstrate compliance with the rules and adopt a privacy-by-design approach. This includes carrying out a privacy impact assessment for high risk processing of data.

- Data Protection Officers: Businesses will be required to designate a Data Protection Officer to monitor compliance with the rules where

  (i) their core activities consist of processing data which requires regular and systematic monitoring of individuals on a large scale, or

  (ii) their core activities consist of processing on a large scale of special categories of data. This includes processing personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health.

- Greater rights for individuals: Individuals will have enhanced rights, such as the right to be forgotten, and businesses should review their procedures to ensure they can comply with these rights.

- Consent of data subjects: A data controller must demonstrate that a data subject's consent to processing of their personal data is freely given, specific, informed and unambiguous.

- Distress claims: The GDPR makes it considerably easier for individuals to bring private claims against data controllers and processors. For distress claims, any person who has suffered "material or non-material damage" as a result of a breach of GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress and hurt feelings even where they are not able to prove financial loss.

- As a result of the GDPR, companies doing business in the EU will be expected to take

extensive steps to ensure personal data held by them is protected and may be exposed to extensive liabilities if they fail to adequately process or safeguard personal data. In addition to the large fines supervisory authorities will be authorised to levy (the insurability of which is open to debate), companies may be liable for any damage caused to individuals. Compliance with the obligation to inform individuals affected by a data breach may also entail significant expenditure.

What is clear is data protection laws within the EU are due to undergo a significant change in the near future. The additional burdens (and associated risk exposure) for data controllers and processors means demand for cyber insurance cover is likely to grow.

However, the General Data Protection Regulation appears to have been drafted without connected vehicles specifically in mind. Personal data is information that can be used to identify a person, whether on its own or with additional information. Information passing from a car to another source will undoubtedly mean there's potential for the driver and possibly passengers, to be identified.

Regulatory frameworks require automotive manufacturers to collect and retain significant amounts of data (e.g. storage of communications data as required under the Data Retention and Investigatory Powers Act 2014). The data obtained by companies can also give rise to specific regulatory obligations to share data (e.g. safety data). These regulatory requirements can sometimes conflict with each other, or with commercial interests of the manufacturers and insurers.

Given that multiple parties are likely to have access to personal data concerning the same individual, joint liability may arise following any mishandling of data. Data protection legislation recognises the possibility of joint control of data, whether it is used for different purposes ("controllers in common") or for the same ends ("joint controllers"). Where a party does not act in accordance with the expected allocation of responsibilities there is a risk joint liability will be incurred. Commercial data sharing agreements between parties will need to take this into account.

Where the data is being accessed by organisations such as garages, insurance companies and service providers, it is possible that upon accessing the data they become 'controllers', as they would be responsible for determining the purpose for processing the data. Under the GDPR they would therefore be required to comply and would be legally accountable for failure to do so.

The impact of the GDPR on manufacturers is that car component design, particularly in relation to connected car technology, will need to accommodate the six principles of data protection 'by design'. Accordingly, hardware and software will need to be configured in such a way that permits a 'controller' to comply with the GDPR. This applies whether the controller is a manufacturer, service centre, insurance company or any other entity which is able to connect to the car.

As an example, hardware and software must be designed to ensure:

- Data which is collected and transmitted is limited to only that which is relevant data for the purpose (second principle)

- Data collected and store by devices on the cars is stored for no longer than is necessary for its purpose (fifth principle)

- Data being stored and broadcast from the car, and its components, is appropriately secured and protected from loss, damage or unauthorised processing (first and sixth principle)

If systems are not able to accommodate the six principles of GDPR, by design and by default, the ability for a 'controller' to use the technology becomes restricted. This is because they too must observe the six principles of GDPR and risk a fine if they don't. This may prevent insurers using connected vehicles systems in some cases, subject to consents from the data subject.

It would therefore be advisable for the Government to consult on the impact of the GDPR, and examine how data controllers and processors will work in the context of connected vehicles. Officials should also examine whether wider standards of consent for the public to agree to their data being used are appropriate and look at the role of data encryption.

The Information Commissioner's Office, the UK data regulator, also needs to produce further guidance on the classification of data on connected vehicles, to clarify the extent of the general public's "right to be forgotten" in this context.

One option available to insurers may be to anonymise or pseudonymise data. This is likely to be expected by consumers and indeed regulators as the default position. Stakeholders should therefore consider building into the design process whether data collected by cars should be held in identifiable or anonymous form. If full anonymization is not possible, then pseudonymisation of the data may be a useful compromise.

Cyber security

In 2015 the National Security Strategy (NSS) reaffirmed cyber threat as a tier one risk to UK interests. The level of threat is considered alongside Terrorism, War and Natural Disasters. Evidence received by the House of Lords Science and Technology Committee highlighted the extent to which connected vehicles will, and already have, been subject to cyber-attacks.

The Committee recommended that the Centre for Connected and Autonomous Vehicles, with involvement from the National Cyber Security Centre, should play a coordinating role with regard to cyber security for connected vehicles. It was also noted the Government should seek to facilitate coordinated international action to tackle the risks associated with cyber security.

On 6 August 2017 the Government issued a new set of guidelines designed to encourage automakers to make vehicles cybersecurity a priority. The guidance, titled "The key principles of vehicle cyber security for connected and autonomous vehicles," consists of eight basic principles.

The Key Principles are an initial step for the Government in regulating this aspect of the automobile industry:

- Principle 1 - organisational security is owned, governed and promoted at board level.

- Principle 2 - security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain.

- Principle 3 - organisations need product aftercare and incident response to ensure systems are secure over their lifetime.

- Principle 4 - all organisations, including sub-contractors, suppliers and potential 3rd parties, work together to enhance the security of the system.

- Principle 5 - systems are designed using a defence-in-depth approach.

- Principle 6 - the security of all software is managed throughout its lifetime.

- Principle 7 - the storage and transmission of data is secure and can be controlled.

- Principle 8 - the system is designed to be resilient to attacks and respond appropriately when its defences or sensors fail.

If an accident or loss occurs as a result of a connected vehicle being hacked then the Government is of the view that it should be treated, for insurance purposes, in the same way as an accident caused by a stolen vehicle. This would mean that an insurer of a vehicle would have to compensate a collision victim for damage caused by hacking but, where the hacker could be traced, the insurer could recover the damages from the hacker. Given the difficulties tracing a hacker capable of infiltrating a connected vehicle would presumably entail, this is likely to be of little comfort to insurers.

Cyber risks present challenges to the insurance and automotive industries. Insurers will need to consider new risks and offer appropriate policies. This will require insureds to meet prescribed standards of security to ensure policies are valid. Manufacturers will need to adapt to these standards and ensure appropriate testing (including penetration testing) and validation so that all components meet the standards before and after integration.

As identified above, several initiatives have led to defining security guidelines and principles in the automotive industry, however these cannot be considered a standard as yet. Indeed the level of detail and requirements are insufficiently precise at present. Accordingly the overall standards landscape has yet to achieve the level of completeness and consistency found in domains such as aircraft safety or smartcard security.

Accordingly, the Government will need to consult on cyber security issues raised by a connected transport ecosystem, to ensure that the unique risks are understood and the appropriate safeguards put in place when the technology is rolled out. The Government should clarify whether connected vehicle operators will be designated as “operators of essential services” within the UK and therefore whether they are required to comply with the NIS Directive, including the developing position in the light of Brexit.

(b) automated driver assistance systems (ADAS);

Automated driver assistance systems are now common in all new vehicles, with many older models also v utilising some form of the technology. Over the last 20 years there has been a move from passive safety to active safety, which has begun the transition to 'assisted' driving, with many elements of the driving process undertaken by the vehicle itself.

These developments have already begun to reduce accident frequency. For example Allianz estimates that 40% of vehicle accidents incurring physical loss or damage occurred during parking or manoeuvring; so ADAS 'Park Assist' will assist in reducing these accidents. Autonomous Emergency Braking, which is now available on nearly every new car and required for a 5* NCAP safety rating, is reducing crash frequency by 20%.

However new risks may be created that drivers and insurance companies are not yet prepared for. This will particularly be the case if drivers are not aware that they need to take control back from the car if sensors fail, which could result in more crashes. Indeed, what is emerging is that insurers are seeing a disproportionate number of repairs following collisions involving vehicles with ADAS capabilities, suggesting overreliance may be being placed on these systems at present. This may as a result of exaggeration in the marketing of ADAS capable vehicles and lack of consumer awareness, which has led to drivers erroneously placing confidence in the vehicle's semi-autonomous abilities. This makes pricing risk difficult for insurers, particularly as these technologies are refined.

International regulators need to urgently deal with the challenges insurers are expected to face as drivers transition from the use of computer-assisted vehicles to those that are automated and driverless. If regulators do not address this, there is a risk that some manufacturers will feel the process is preventing development and seek ways to circumvent the regulatory regime as some have appeared to do already (Tesla's autopilot being a prime example). It is therefore vital that regulation keeps pace so that the rollout of automated technology can be managed safely.

As technology shifts from driver assistance to fully automated systems, liability is likely to be determined by the extent to which the driver is expected to remain in control of the vehicle. However, the liability position during the "handover" period between driver and autonomous modes remains unclear. Liability could be shared between the driver, manufacturer, software provider, software engineer and vehicle data provider in such circumstances.

Insurers see two clear levels of automation; those that support the driver (Assistance) and those that fully automate control (Automated). The insurance industry believes a vehicle should only be sold to the public as an ‘automated’ vehicle when it reaches a level of automation where a driver can safely disengage in the knowledge that the car has sufficient capabilities to deal with virtually all situations it may encounter on the road, avoid almost all conceivable crash types and continue to function adequately even in the event of a partial system failure (levels 4 and 5).

If regulators allow the development of vehicles that could be described as level 3, then the insurance industry proposes that these should only be permitted with high levels of robustness and redundancy that largely mimic Level 4 functionalities.

A list of minimum system requirements have been defined that:

- Maximise safety benefits by requiring speed limit and safe following compliance.

- Minimise risks, for example strict hands-on controls, three strikes (hands-on warnings) and you're out and a safe stop at the side of the road capability.

Vehicle manufacturers are very keen to bring automated driving technology to market as quickly as possible and many claim they already have systems that are capable. It is questionable whether the current process of regulatory development can produce the necessary range of new and amended technical requirements sufficiently quickly.

The ABI has noted that it is appropriate that regulators consider alternative regulatory approaches for automated driving concurrently with assisted systems and that these new regulations should:

- Develop rapid and robust technical requirements e.g. ensuring fully redundant systems;

- Be available to guide vehicle manufacturers as soon as possible: prevent unregulated systems being sold as Automated where they require driver intervention to be safe;

- Be designed and categorised as automated vehicles and be capable of recording event data that allows both insurers and vehicle manufacturers the unambiguous identification of liability.

Vehicles developed which require the driver as part of their back-up redundancy (Levels 2 and 3) should therefore not be considered to be 'automated vehicles' and the provisions of the Automated and Electric Vehicles Bill would not apply.

The insurance industry is highly supportive of ADAS at Levels 1 and 2, where they act only in the brief moments before a collision or where they act only to support and not replace driver inputs. However, at Level 3 the driver is not needed for the driving task but must be capable of resuming control at any moment. The technology in production that is approaching that level, and the systems currently under development, have diverse capabilities and widely differing user interfaces which require standardisation and appropriate regulation.

The ABI notes there is significant potential for public confusion around the responsibilities of the driver of such vehicles and a wide variation in the level of risk associated with each vehicle. This will make the accurate pricing of insurance for these vehicles very difficult. Analysis suggests that the total number of claims will probably be lower on aggregate with these technologies, because they are sold with the benefits of more sophisticated pre-crash ADAS that will be active on all roads even during manual driving.

However, the analysis also suggests a risk of an increase in collisions on motorways during highly assisted driving where both system and an inattentive driver miss unusual hazards that would still be obvious to an alert driver, and where systems execute stops in live running lanes because their driver is unresponsive. The proportion of catastrophic claims in these collision types may be higher than most crashes and these can be extremely damaging to individual insurers and the wider reputation of automation, potentially setting back market adoption significantly. Where insurers are concerned that the risk of having to deal with consequences of these catastrophic claims is too high, they may be reluctant to offer cover for these vehicles, even when their impact on the overall volume of road accidents is positive.

However, insurers accept that some sections of the vehicle manufacturing industry see the technologies at Level 3 as vital stepping stones in the development of full automation. If this incremental development approach is to be permitted then insurers consider that strict controls are necessary in both the type approval regulations governing the construction of new vehicles and the national legislation governing how vehicles are permitted to be used.

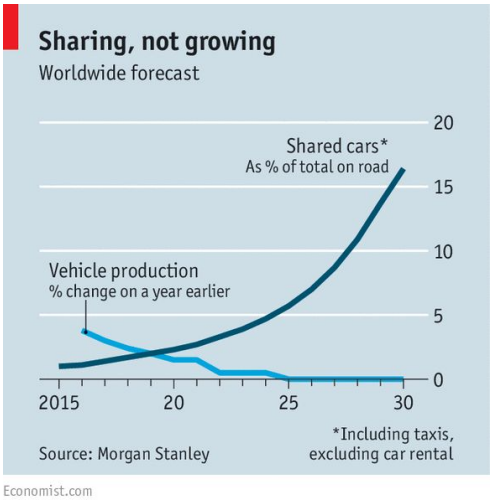
Insurers propose a two-step approach that allows the development of robust regulations regarding assisted driving systems whilst allowing the parallel definition of less prescriptive "light touch" regulations surrounding automated driving. This will help to ensure the rapid proliferation of automated systems to deliver the perceived benefits, whilst ensuring vehicle manufacturers, frustrated with the current complex regulatory system, are not allowed to sell inferior technology to gain technical lead.

The legal system will need to acknowledge and respond to these changes. If drivers are permitted to rely on automated technology then it is likely that the present 'reasonable motorist' test will continue to apply. For example motorists have an obligation to keep a reasonable distance from the vehicle in front and accordingly the same test could apply to technology. If the driverless car has failed to perform this function and not kept a proper lookout for the vehicle in front, then there is no impediment to finding fault in respect of that vehicle.

The law must therefore develop to acknowledge the greater reliance that the driver is placing on this technology. Currently for example if a pedestrian was hit whilst a vehicle was reversing using its automated parking function, neither the driver nor the pedestrian would be able to rely upon this technology to negate their liability. As the technology develops, the driver may seek to argue that an element of fault lies with the manufacturer and seek a contribution of liability.

However in the future, if the very same accident occurred in a fully autonomous vehicle then it is likely that the manufacturer or software provider would be considered to be at fault. Indeed the onus may change to the software provider to demonstrate, for example, that the driver had failed to install a software upgrade rendering the parking function useless and thus be able to make a contribution claim from the driver.

(c) car/ride sharing;



The UK is following the global trend that has witnessed motor vehicles begin to become a commoditised public service. Car clubs such as ZipCar already offer cars without ownership, while services such as Uber and Lyft provide on-demand transport solutions.

Car sharing will certainly bring about changes in urban driving, driver behaviour, and the business models of manufacturers and insurers. It will expose new revenue pools and become increasingly relevant to a cohort of mostly younger urban drivers. However, until the move to fully automated vehicles, it is unlikely to be materially disruptive to the status quo for insurers.

Two forms of car sharing operate in the UK. The first is the fleet model, in which an organisation purchases and insurers a large fleet of vehicles for use by consumers. The other is peer-to-peer car sharing, where an Individual uses a peer-to-peer company that acts as a broker and often insures the vehicle also, although the motor insurance industry has also responded to this developing market.

Insurers will commonly cover car sharing for the owner as long as the policy holder is not profiting from the hire of their vehicle. Anyone making a regular profit out of sharing would need specialist cover. Under normal circumstances the carriage of passengers for fares is classed as “hire or reward” and is subject to either Public Service Vehicle (PSV) Hackney Carriage or Private Hire Car licensing laws. Car schemes and car-sharing are specifically exempted from such requirements by law under the Public Passenger Vehicle Act 1981.

On demand (pay per use) policies are currently being offered by the market, employing telematics to monitor driver use. As a result coverage is increasingly more focused on driving habits with usage-based insurance (pay how you drive) or becoming more centred on a pay-per-mile basis.

Car/ ride sharing motorists will need to comply with all the legal requirements of everyday motoring, including ensuring the driver and vehicle is properly licenced and the driver is insured. The vehicle must be kept in roadworthy condition and should comply with the relevant “Construction and Use” regulations in respect of lights, brakes, steering, exhaust, wipers, washers etc. (Road Vehicles (Construction and Use) Regulations 1986).

The vehicle should be driven safely and with consideration for all other road users, i.e. in accordance with the Highway Code. A failure on the part of a person to observe any provision of the Highway Code shall not of itself render that person liable to criminal / civil proceedings of any kind, but pursuant to the Road Traffic Act 1988 any such failure may in any proceedings may be relied upon by any party to the proceedings as tending to establish or negate any labiality which is in question in those proceedings.

Liability is one of the most significant issues for personal auto insurers. Who pays if the car is involved in an accident while participating in car-sharing? Some car-sharing companies are facing this challenge by offering primary coverage in the event of an accident; some are offering comprehensive and collision coverage; and some are even offering third-party liability coverage.

Peer-to-Peer car sharing presents a potential difficulty for insurers. If the vehicle user (as opposed to the vehicle owner) is uninsured, insurers will commonly retain a liability for losses arising from accidents caused by the user under the Road Traffic Act. Improved regulation of this section of the sharing economy may be needed, particularly for peer-to-peer arrangements in use without a central coordinating organisation, where lack of proper governance and risk management is likely to be more common.

The claims experience is also a potential problem for insurers. Proving fault or even who was driving at the time of the alleged accident, with the associated issues of fraud is pervasive in this area. To help alleviate the difficulty, some peer-to-peer businesses are developing data recorders and phone apps to track mileage, time and who is driving the vehicle. This raises significant data protection issues akin to those discussed in Question 3.

(d) Alternative fuel vehicles

Alternative fuel vehicles are to become imperative in the UK following the announcement that Britain is to ban all new petrol and diesel vehicles from 2040 on public health grounds. The Government is in the process of outlining its plans to fulfil its aim for nearly all cars and vans on UK roads to be zero emission by 2050.

The Automated and Electric Vehicles Bill introduces a regulatory framework to keep pace with the fast-evolving technology for electric cars and includes provision for electric charging points and hydrogen refuelling stations at motorway service areas and large fuel retailers.

A new £23 million fund to accelerate the take up of hydrogen vehicles and roll out more cutting-edge infrastructure has been announced by the government in March 2017. Hydrogen fuel providers will be able to bid for funding in partnership with organisations that produce hydrogen vehicles to help build high-tech infrastructure, including fuel stations. The funding is hoped to boost the creation of hydrogen fuel infrastructure and uptake of hydrogen-powered vehicles.

Electric vehicles are expected to reach total cost of ownership parity with petrol vehicles sooner than expected, possibly by 2018, which could see a surge in the number of electric vehicles on UK roads. UBS for example has increased its electric vehicles sales estimates globally by 50% and predicts a third of all cars sold in Europe will be electric or hybrid by 2025.

However whilst the sales of electric and plug-in hybrid vehicles have increased from 2,000 vehicles in 2012 to 86,000 in 2016, the number of charging stations available is still far behind with 11,700 in 2016. The Government intends to redress the balance by ensuring that every motorway service station and large petrol station has charging facilities but this will come at a significant cost. A single basic charge point will cost around £1,400 whilst a rapid charger will cost £22,000 to install. This raises capacity issues and whether the UK's developing infrastructure will be able to cope with material increases in demand.

The cost of charging stations isn't the only concern. A study carried out by Green Alliance has found just six electric cars charging at the same time on a street could cause local power shortages. The Government will be required to invest in public charging infrastructure in order to handle the future uptake of electric vehicles. New and improved batteries could be the answer to reducing the usage of charging points at one time. Bosch is currently developing a lithium-ion solid state battery that they hope will double the range of electric vehicles at half the cost of today's batteries.

Electric vehicles are likely to be a more cost effective option for UK motorists as the introduction of new technology each year means the value often depreciates faster and the majority of electric cars are exempt from the road and congestion charges. But whether electric vehicles will see an increase in costs for insurers following an accident remains to be seen.

Whilst it is potentially cheaper to repair and maintain electric vehicles, as they have fewer mechanical components, there is a possibility that it could be more expensive if a specialist mechanic / engineer is required. There is likely to be a shortage of knowledge and expertise required to develop a consistent repair network for insurers, prompting the Institute of the Motor Industry to call for the government to invest £30 million into training technicians in specialist electric and hybrid vehicle repair.

Insurance policies are already in place for electric vehicles. Direct Line offers e-car insurance which is similar to regular car insurance but takes into consideration unique issues such as costs of specialised parts, repairs conducted by specialist mechanics, expensive batteries and potentially greater risk of pedestrian accidents due to quiet running. Insurers may not provide cover for batteries that are leased from manufacturers for example and new policy wordings will be required for this emerging technology. Policies covering accidents resulting from charging outlet cables in public areas may also begin to be seen, raising issues of pricing risk for insurers for what is still a developing technology.

Supporting materials and links to relevant sources

- Automated and Electric Vehicles Bill & Explanatory notes

https://publications.parliament.uk/pa/bills/cbill/2016-2017/0143/cbill_2016-20170143_en_1.htm

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/620838/Queens_speech_2017_background_notes.pdf

https://publications.parliament.uk/pa/bills/cbill/2016-2017/0143/en/17143en.pdf

- Road Traffic Act 1988

http://www.legislation.gov.uk/ukpga/1988/52/contents

- Vehicle Technology and Aviation Bill

http://services.parliament.uk/bills/2016-17/vehicletechnologyandaviation.html

- Automated vehicle Consultations documentation

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/603887/connected-autonomous-vehicles-uk-testing-ecosystem-government-response.pdf

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/581577/pathway-to-driverless-cars-consultation-response.pdf

https://www.gov.uk/government/consultations/advanced-driver-assistance-systems-and-automated-vehicle-technologies-supporting-their-use-in-the-uk

https://www.gov.uk/government/consultations/driverless-vehicle-testing-facilities-call-for-evidence

https://www.gov.uk/government/publications/driverless-cars-in-the-uk-a-regulatory-review

https://www.gov.uk/government/consultations/driverless-cars-regulatory-testing-framework

- Consumer Protection Act 1987 http://www.legislation.gov.uk/ukpga/1987/43/contents

- Centre for Connected and Autonomous Vehicles

http://www.csap.cam.ac.uk/organisations/centre-connected-and-autonomous-vehicles/

- ABI and Thatcham Consultation response

https://www.abi.org.uk/globalassets/sitecore/files/documents/consultation-papers/2016/09/090916_abi_thatcham_response_ccav_automated_driving_consultation.pdf

- Space Industry Bill & Guidance notes

https://publications.parliament.uk/pa/bills/lbill/2017-2019/0007/18007.pdf

https://publications.parliament.uk/pa/bills/lbill/2017-2019/0007/18007en06.htm

- Principles of cyber security for connected and automated vehicles

https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles

- Regulating automated driving - the UK insurer view

https://www.abi.org.uk/globalassets/files/publications/public/motor/2017/07/regulating-automated-driving/

- Adrian Flux driverless cars insurance policy

https://www.adrianflux.co.uk/driverless-cars/driverless-car-insurance-has-arrived/

https://www.adrianflux.co.uk/pdfs/documents/driverless-car-insurance-policy-document.pdf

- Data Protection Bill – Statement of Intent

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635900/2017-08-07_DP_Bill_-_Statement_of_Intent.pdf

- Public Passenger Vehicles Act 1981

https://www.legislation.gov.uk/ukpga/1981/14/contents

- House of Commons briefing paper - Electric vehicles and infrastructure

http://researchbriefings.files.parliament.uk/documents/CBP-7480/CBP-7480.pdf

- Data Retention and Investigatory Powers Act 2014

http://www.legislation.gov.uk/ukpga/2014/27/contents/enacted

- Automobile Insurance in the era of autonomous vehicles – White Paper

https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/id-market-place-of-change-automobile-insurance-in-the-era-of-autonomous-vehicles.pdf

- National Security Strategy and Strategic Defence and Security Review 2015

https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015

II. CYBER RISKS

5. a Identify the concerns that have emerged in your jurisdiction as a result of cyber risks.

Cyber risk is a hot topic and with good reason. As organisations and society as a whole become ever more interconnected and reliant on technology (for example, with the "Internet of Things" and use of the "cloud"), this inevitably leads to greater exposure to cyber risks, especially when coupled with a global increase in cyber-related crime moving into the mainstream and the prevalence of agile working.

As numerous surveys show, the number of cyber events suffered by UK companies is on the increase. The UK Government's Cyber Security Breaches Survey 2017 revealed that nearly all UK businesses surveyed are exposed to cyber security risks. Just under half (46%) of all UK businesses surveyed identified at least one cyber security breach or attack in the last 12 months. This rises to two-thirds among medium firms (66%) and large firms (68%). The most common types of breaches related to staff receiving fraudulent emails (72% of those who identified a breach or attack), followed by viruses and malware (33%), people impersonating the organisation online (27%) and ransomware (17%).

Data privacy and protection is a key cyber risk in the UK and data protection laws are toughening as a result (discussed in more detail in section 5b). Other concerns are the risk to critical systems (seen recently with the WannaCry attack on the National Health Service (NHS)) and infrastructures, such as breaches in the energy sector. A growing concern is the business interruption and supply chain impact a cyber event could have, which in some instances could outweigh the direct losses that are incurred. Reputational risk is also a growing concern.

The extent of the risk to UK organisations is difficult to quantify as a lot of incidents remain unreported but there is no doubt that incidences are increasing. Given the ever-evolving nature of the risk, it is a case of "if" not "when" an incident will occur.

5. b Is there any legislation in place or under consideration that might affect such risks?

Legal liability could arise as follows:

- Statutory, contractual and tortious claims from those who have suffered damage and/or distress caused by the unlawful acquisition, disclosure and/or use of their personal information;

- Criminal or regulatory actions for non-compliance with legal obligations to ensure information and networks are secure or, in certain circumstances, for failing to respond effectively to a cyber event.

In the UK, the existing legal framework (as at November 2017) relevant to the above consists of various instruments derived from the EU regulatory framework for electronic communications and cybersecurity. This framework is set out in Appendix A. The framework is changing and this is explored in more detail in the following sections.

Current cyber security/data protection laws

The current UK cyber security/data protection law is comprised of various statutes, some implementing the current EU regulatory framework and others specific to the UK. The primary

sources are:

(a) Data Protection Act 1998

(b) Privacy and Electronic Communications (EC Directive) Regulations 2003

(c) Communications Act 2003

(d) Computer Misuse Act 1990

(e) Official Secrets Act 1989

(f) Regulation of Investigatory Powers Act 2000

(g) Freedom of Information Act 2000

(h) Human Rights Act 1998

Brief details on (b)-(h) can be found in Appendix B. The Data Protection Act 1998 (DPA) is in force until the General Data Protection Regulation (GDPR), implemented in the UK via the (currently draft) Data Protection Bill (DPB), comes into force on 25 May 2018. The focus of this section will therefore be on the DPB and the GDPR. Details of the DPA can be found in Appendix C.

Incoming cyber security laws

General Data Protection Regulation/Data Protection Bill

UK data protection law will change on 25 May 2018 when the GDPR takes effect. The Government has confirmed that the GDPR will apply in the UK irrespective of Brexit The Government recently published a statement of intent in which it proposed a new Data Protection Bill which implements the GDPR in full whilst also exercising a number of agreed modifications to the GDPR to make it work for the benefit of the UK in areas such as academic research, financial services and child protection. It is therefore important the GDPR and the Bill are read side by side. In addition to the GDPR provisions, the DPB also covers:

- processing that does not fall within EU law, for example, where it is related to immigration;
- implementation of the EU's Law Enforcement Directive, which is separate from the GDPR;
- as national security is outside the scope of EU law, the Government has inserted provisions requiring the intelligence services to comply with internationally recognised data protection standards, based on Council of Europe Data Protection Convention 108;
- provisions setting out the Information Commissioner's Office's (ICO) duties, functions, powers and enforcement provisions.

The DPB is currently making its way through Parliament. At the time of writing, the DPB is expected to have its second reading in the House of Commons on a date yet to be determined. The progress of the DPB and corresponding documents can be viewed on the Parliament website here.

The GDPR places obligations upon those who deal with data and it confers broad rights upon those whose data is processed. The GDPR/DPB includes a number of wide-ranging changes to data protection law which will impact on cyber risks, including:

- Tougher fines: Businesses will be subject to fines of up to €20 million or 4% of annual global turnover, whichever is higher, for infringements with some of the rules (clause 150 DPB);

- 72-hour data breach notifications: A data controller must notify the relevant supervisory authority of a personal data security breach within 72 hours of becoming aware of the breach. They may also be required to inform the affected individuals where there is a high risk to their personal data (clause 65 DPB);

- Accountability and privacy-by-design: Businesses will be required to demonstrate compliance with the rules and adopt a privacy-by-design approach. This includes carrying out a privacy impact assessment for high risk processing of data (clause 101 DPB);

- Data Protection Officers: A data controller must designate a data protection officer, unless the controller is a court, or other judicial authority, acting in its judicial capacity (clause 67 DPB);

- Greater rights for individuals: Individuals will have enhanced rights, such as the right to be forgotten and access to their data;

- Consent of data subjects: A data controller must demonstrate that a data subject's consent to processing of their personal data is freely given, specific, informed and unambiguous;

- Distress claims: Distress claims have been codified; any person who has suffered "material or non-material damage" as a result of a breach of GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The DPB also provides for non-material claims, as "damage" is defined in the DPB (clauses 159 and 160) as including "financial loss, distress and other adverse effects, whether or not material."

As a result of the GDPR/DPB, companies doing business in the EU will be expected to take extensive steps to ensure personal data held by them is protected and may be exposed to extensive liabilities if they fail to adequately process or safeguard personal data. In addition to the large fines, supervisory authorities will be authorised to levy (the insurability of which is open to debate), companies may be liable for any damage caused to individuals. Compliance with the obligation to inform individuals affected by a data breach may also entail significant expenditure.

What is clear is data protection laws are due to undergo a significant change in the near future. The additional burdens (and associated risk exposure) for data controllers and processors means demand for cyber cover is likely to grow.

Network and Information Security Directive (NIS Directive)

This Directive is aimed at increasing and improving cooperation between member states. It imposes obligations on operators of essential services and digital service providers to take appropriate and proportional technical and organisational measures to manage risks to networks and information systems, and to take appropriate measures to prevent and minimise the impact of incidents. Incidents having a significant impact on the continuity of services must be notified to the regulator.

On 8 August 2017, the Government released a statement confirming the UK's intention to support the aims of the NIS Directive and released a consultation for the proposed implementation into UK law. The consultation states that service providers operating in the following sectors should qualify as an “essential service”: energy, health, digital and transport (air, road and maritime). The UK needs to put in place a framework of institutions to facilitate the operation of the NIS Directive. The consultation states "The elements of this national framework include:

- adopting a national strategy on the security of network and information systems;
- designating “one or more national competent authorities” to oversee implementation and compliance with the Directive’s provisions;
- designating a “single point of contact” to act as a liaison point with other Member States; and
- creating one or more computer security incident response teams (CSIRTs)."

The consultation closed on 30 September 2017. At the time of writing, the Government is currently analysing the feedback it received. A formal response is expected by 11 December 2017 (10 weeks from the consultation closing date).

The Government issued a formal response to the consultation feedback on the 28th January 2018: https://www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive

The Government received over 350 responses to its consultation.

The main changes the Government proposes to make are in clarifying:

- the thresholds required to identify operators of essential services;
- the role of the Competent Authority and how powers may be delegated to agencies;
- that the role of the National Cyber Security Agency is limited to cyber security;
- the expectations on operators within the first year or so; and
- the definitions of Digital Service Providers.

The Government also intends to simplify:

- the incident response regime, to separate incident response procedures from incident reporting procedures; and
- the penalty regime slightly, to reduce the risk of fines in excess of £17m.

The Government believes these changes will provide further reassurance to industry. The Government again reiterates that their approach will remain reasonable, proportionate and appropriate and that the Government and Competent Authorities will work closely with industry to ensure that this legislation will be a success.

Full consultation response can be read here.

6. How has the insurance industry responded to cyber risks? In particular:

(a) do property policies cover losses from cyber risks, or is special insurance required?

(b) is insurance and reinsurance readily available?

(c) are there any special restrictions imposed on cyber risks, e.g. event limits or deductibles?

Overview of the cyber insurance market

Cyber insurance is a fast-growing sector in the UK insurance market. Lloyd's of London has reported that the market saw a 50% surge in policies in 2016 and it forecast a further growth in 2017 and the coming years.

Businesses across all sectors are beginning to recognise the importance of cyber insurance in today's increasingly complex and high risk digital landscape. The additional business risks arising from the GDPR/DPB mean organisations will increasingly seek cover in the cyber insurance market and will want to assess whether the large fines that can be imposed are recoverable on their insurance. Insurability of fines and penalties is an area fraught with complexity and affected by matters of public policy. This complexity is particularly relevant to cyber insurance, given many cyber insurance policies will cover fines and penalties to the extent they are "insurable at law". There is currently no UK precedent which establishes how a fine flowing from a breach of data protection legislation may be treated. The ICO does not expressly prohibit the insuring of fines, unlike the UK's Financial Conduct Authority (FCA), for example, which expressly prohibits the insuring of fines and penalties they impose. However, the GDPR/DPB focuses on the nature of the conduct in question when considering whether to impose a fine and provide that when fines are assessed, the nature of the conduct will be taken into account setting the level of the fine. There may therefore be the possibility that the most serious fines under the GDPR/DPB will not be recoverable, but each case will of course turn on its own facts.

The fact the GDPR will create a harmonised data protection regime within the EU should enable insurers wishing to offer cover for this type of risk to do so with a degree of confidence. The "one-stop shop" concept in particular should obviate the need for insurers to conduct an assessment of the data protection regime for every single EU member state in which a proposed insured operates.

However, the market is still in its infancy and despite the growing awareness from organisations about cyber risk, plus the surge in uptake of cyber insurance, the Government's Cyber Security Breaches Survey 2017 found that only 38% of firms surveyed said they have insurance covering a cyber security breach or attack (though this figure is higher for larger organisations). The report notes as follows:

"The qualitative survey shows there are very disparate levels of awareness around cyber insurance. Some businesses – typically smaller ones – were simply not aware of the notion at all, while others had looked into it in depth and ruled it out, or were still looking for an appropriate policy…The larger businesses that had looked into it had mixed impressions about the policies available, and felt that the insurance market still needed to evolve before it became viable for most firms."

Cyber insurance coverage

Cyber insurance coverage may be contained in a stand-alone policy, as a specific endorsement on existing policies (e.g. as an extension for specific losses to a property policy) or as part of traditional policies without a specific endorsement ('silent cyber coverage', discussed in more detail below).

The stand-alone cyber insurance market largely emerged in response to the increasing prevalence of exclusions for cyber losses in policies such as property, kidnap and ransom, general liability, professional indemnity and other traditional insurance policies.

Exclusions in these policies can be of a general nature, excluding all losses resulting from a cyber event or excluding specific losses, such as liability related to data breaches. Triggers on traditional policies, for example the need for property damage in order to recover for business interruption losses, led to gaps in coverage.

Stand-alone cyber insurance aims to reduce/close these gaps in cover. Scope of cover can vary and can include some or all of the following:
The scope of cover, including typical limits on the cover is set out in more detail in Appendix D.

The challenge is for wordings to keep pace with the ever-evolving risk to ensure insurers are covering what they intend to cover and insureds get what they hope they are paying for.

As noted above, cyber risks can also be covered by traditional policies, such as property and general liability policies. Sometimes specific endorsements are agreed between the insurer and insured but often there is a 'silent' or 'non-affirmative' cyber risk inherent in traditional policies.

The Prudential Regulation Authority (PRA) recently published a final Supervisory Statement setting out its concerns and expectations of firms in relation to cyber risk (SS4/17). The PRA has significant concerns about the loss potential of ‘silent’ (or ‘non-affirmative’ as it was re-coined) cyber risk – the cyber risk inherent in policies insurers underwrite, aside from cover expressly provided for such in cyber insurance policies – and the management of this risk. In particular, the PRA notes that casualty (direct and facultative), marine, aviation and transport (MAT) lines of business are potentially significantly exposed to ‘silent’ cyber losses.

The PRA proposes that firms review how they underwrite risks in order to mitigate the ‘silent’ cyber risk effectively. Various suggestions are made as to how to achieve this, such as: making adequate capital provisions linked with the risk; adjusting the premium to reflect the additional risk and offer explicit cover; introducing robust wording exclusions; attaching specific limits of cover; and offering cyber cover at no extra premium when the board has confirmed that a particular line of business does not carry material ‘silent’ cyber risk and is in line with the stated risk appetite.

From an insured's perspective, the Government's Cyber Security Breaches Survey 2017 found there is mixed understanding of what cyber insurance may or may not cover, with just 18% feeling they understand their policy well. Contributing to this lack of understanding, is the often held belief amongst organisations that they are covered for cyber risks through a more general indemnity insurance policy. As noted above, traditional policies may provide cover (even where this was not intended) but organisations run the risk that they find themselves without appropriate cover in the event of a cyber incident. Looking at professional indemnity policies (PII), for example, these are designed to cover failures to act with reasonable skill and care and are triggered by acts relating to the provision of professional services. Further, PII covers professionals for losses incurred by liability

to third parties. As such, they would not respond to first party losses incurred in dealing with a cyber event, possibly leading to coverage disputes with insurers.

The market is still in its infancy and more needs to be done on both sides. For insurers, the PRA further proposes that firms establish, and regularly review strategies from the top down as to how to manage the risk and that organisations clearly demonstrate risk appetites. This should include producing internal management information approved by the board. The PRA also expects firms to demonstrate that they are committed to understanding and developing their knowledge of cyber insurance risk and to invest in developing cyber risk talent. For insureds, the lesson is effective risk management, through the implementation of appropriate policies, procedures and training, alongside the purchase of stand-alone cyber insurance.

APPENDIX A

CURRENT EU CYBERSECURITY FRAMEWORK

- **The Framework Directive (2002/21/EC) as amended by the Better Regulation Directive (2009/140/EC)** provides a common regulatory framework for telecoms providers who supply electronic communications networks or services to the public. Essentially the directive captures all forms of communications transmission technology. It requires providers to meet a network security standard and to notify the competent regulatory authority of breaches that have a significant impact on the operation of the network.

- **The Directive on Privacy and Electronic Communications (2002/58/EC) as amended by the Citizens' Rights Directive (2009/136/EC)** Concerns the processing of personal data and the protection of privacy in the electronic communications sector. It contains a number of important cybersecurity obligations, including a security measures obligation pursuant to which providers of electronic communications systems must: (i) take appropriate technical and organisational measures to protect their services; and (ii) notify, without undue delay, the competent national data protection authority of a personal data breach along with the relevant individuals when the breach is likely to adversely affect their personal data or privacy.

- **The Notification Regulation (611/2013)** Clarifies and confirms actions that the electronic communications sector in the EU must take if their customers' personal data is lost, stolen or otherwise compromised.

- **The Data Protection Directive (95/46/EC)** broadly, the purpose of the Data Protection Directive was to harmonise national data protection laws throughout the EU. It introduced an extensive data protection regime for the EU by imposing broad obligations on those who collect personal data (data controllers) as well as conferring broad rights on individuals about whom data is collected (data subjects). It was implemented in the UK by the Data Protection Act 1998.

APPENDIX B

UK LEGISLATION

- **The Privacy and Electronic Communications (EC Directive) Regulations 2003** Implements the e-Privacy Directive (as amended) into UK law. It contains provisions that govern (among other things) direct marketing by email and/or when using SMS. Imposes obligations on public electronic communications service (PECS) providers to take appropriate technical and organisational measures to safeguard the security of its services. Mandatory notification requirements.

- **The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011** obliges organisations using cookies (which includes equivalent technologies) only to place cookies on the machines of users who have given their consent.

- **The Communications Act 2003 (**Section 105A-105D) implements Article 13a of the Framework Directive into UK law. It imposes obligations on public electronic communications network (PECN) providers and public electronic communications service (PECS) providers to implement technical and organisational measures to manage security risks. It also imposes notification obligations.

- **The Computer Misuse Act 1990** Sets out cybercrime offences e.g. for unauthorised access or interference with a computer.

- **The Official Secrets Act 1989** sets out offences, largely applying to public sector servants and contractors, criminalising the disclosure of or failure to secure information which is damaging to the armed forces, security or intelligence services (or their work) or endangers the lives of British citizens abroad or is damaging to the UK's interests abroad.

- **The Regulation of Investigatory Powers Act 2000** Regulates, among other matters, the interception of communications on a public or a private network.

- **The Freedom of Information Act 2000** Provides for general rights of access to “recorded” information held by public authorities.

- **The Human Rights Act 1998** though it is not directly enforceable against private organisations, it does require a court or tribunal to interpret any UK legislation in a way that is compatible with the rights set out in the HRA. This means that, where appropriate, courts and tribunals must consider individuals’ privacy rights.

APPENDIX C

DATA PROTECTION ACT 1998

The Data Protection Act 1998 (DPA) implements the Data Protection Directive (95/46/EC) and will apply until 25 May 2018.

In very general terms, the DPA applies to the "processing" of "personal data", both of which terms are very widely defined: "personal data" is data which relates to an individual, which might affect the individual's privacy and is biographical by nature and "processing" is broadly defined to include obtaining, recording, holding, using, disclosing or erasing data (section 1(1), DPA). In effect, any activity involving personal data will fall within its scope. This means that practically any business operating in the UK, which holds information about individuals (whether employees, customers or anyone else) is affected by the DPA. Since breaches of data protection laws can result in criminal as well as civil liability (not to mention adverse publicity, which is increasingly the likely result of non-compliance), no organisation can afford to ignore its data protection obligations.

Perhaps the key feature of the DPA (section 4) is the "*duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller*". These principles provide the skeleton around which the regulatory framework is formed.

DPP	Text
1	Personal data shall be processed fairly and lawfully and, in particular shall not be processed unless – (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met
2	Personal data shall be obtained only for one or more specified and lawful purposes
3	Personal data shall be adequate, relevant and not excessive
4	Personal data shall be accurate and, where necessary kept up to date
5	Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
6	Personal data shall be processed in accordance with the rights of data subjects
7	Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction of, or damage to, personal data.
8	Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

The DPA Regime is enforced and overseen by the ICO, which regularly provides guidance on interpretation. Its edicts on organisational compliance inform, or at least they should inform, the policies and actions of the entities that are subject to the rules.

The ICO has the power to impose a fine (up to a maximum of £500,000) for serious contraventions of the DPA (section 55A). Before doing so, the ICO must be satisfied that the contravention was serious and was of a kind likely to cause substantial damage or substantial distress, and that the data controller either:

- Deliberately contravened the DPA 1998; or

- Knew or ought to have known that there was a risk the contravention would occur, and that it would be likely to cause substantial damage or distress, but still failed to take reasonable steps

to prevent it from happening.

The ICO will take into account the sector, size, and financial and other resources of a data controller or person, as it is not the purpose of a penalty notice to impose undue financial hardship on an otherwise responsible person.

There is currently no general legal obligation for an organisation to notify the ICO of a breach of personal data. However certain pieces of legislation do provide for mandatory notification in the event of personal data breaches: for example, the Privacy and Electronic Communications Regulations 2003 states that "service providers" must notify the ICO of a data breach within 24 hours of becoming aware of the essential facts of the breach. A "service provider" means someone who provides any service allowing members of the public to send electronic messages. This includes telecoms providers and internet service providers. The ICO considers voluntary notification to be a mitigating factor when considering the level of monetary penalty to be imposed.

Where there is no specific requirement to do so, the ICO will expect organisations to report “serious breaches” (taking into account the potential detriment to data subjects, the volume of personal data lost, released or corrupted and the sensitivity of the data lost, released or corrupted). Equally, unless a more specific legal requirement applies, there is no legal obligation to notify affected individuals unless the ICO orders an organisation to do so.

In addition to regulatory fines, section 13 of the DPA allows individuals affected by a breach of the DPA to recover compensation from the data controller. Section 13(1) as drafted provides that an individual who suffers “damage” by reason of a contravention of the DPA is entitled to compensation from the data controller for that damage. The courts had previously interpreted "damage" as meaning pecuniary loss: for example if personal data is lost as a result of a hack and the individuals involved fell victim to identity fraud as a result, section 13(1) would entitle them to claim for the financial loss suffered (as long as they can also prove a breach of the DPA). Section 13(2) said that where an individual suffers distress as a result of the breach, they can only recover for that distress where they also suffer damage (i.e. a financial loss) or where the data is processed for the special purposes.

The section was effectively rewritten by the case of *Vidal-Hall v Google Inc* [2015] which concerned Google's collection of browser generated information about individuals’ internet usage by using cookies that then enabled advertisers to select adverts targeted or tailored to the individuals to appear on their screen. The claim was brought by three individuals who claimed that this practice revealed private information about them which could be seen on their screens by third parties. This allegedly caused them distress, but no financial loss.

The Court held that section 13(2) of the DPA did not properly incorporate into UK law the provisions of the underlying EU legislation on which the DPA is based – it was incompatible with Article 23 of the Data Protection Directive. The Court therefore effectively re-wrote section 13 with the result that if an individual suffers distress as a result of a breach of the DPA, it can recover that distress from the data controller.

Other potential statutory causes of action following a cyber event include:

- Potential for a section7 Human Rights Act 1998 claim for breach of Article 8 of the European Convention on Human Rights (right to respect for private and family life);

- Copyright, Designs and Patents Act 1988 for copyright infringement;

- Trade Marks Act 1994 for trademark infringement;
- Defamation Act 2013 for libel/slander (also actionable as a tort)

APPENDIX D

SCOPE OF COVER

Privacy and Confidentiality Breach Cover	Cover for losses arising out of actual disclosure of any personal data via computer systems. Some polices cover for suspected disclosure (on the basis that it is not always possible to definitely say if a particular person's information has been disclosed). The cover is intended to pick up privacy liability claims arising out of invasion of privacy of the individual and breach of privacy-related legislation e.g. DPA 1998 which may arise under English law: ● Claim for compensation under section 13 DPA ● Breach of confidence, arising from breach of equitable obligations of confidentiality ● Misuse of private information – see *Vidal Hall v Google Inc* which confirmed that misuse of private information is actionable as a common law tort ● Breach of contract e.g. breach of an express or implied term that data would be stored securely and with due care ● Negligence e.g. failure to take reasonable security precaution when storing customer data
Network Security Cover	Failure of network security can lead to many different exposures, including a consumer data breach, destruction of data, virus transmission and cyber extortion. These can lead to third party exposures. Network security coverage can also apply if you're holding trade secrets or patent applications for a client, and that information is accessed due to a failure of your security. Claims can arise, for example, out of a hacker/employee utilising without authorisation the computer network to commit fraud, theft or DDoS attack and/or transmission of viruses (inadvertently or by employee with vendetta for example) and may be advanced under English law under contract or tort law.
Media Liability Cover	To cover defence costs and civil damages arising from defamation, breach of IP rights, breach of privacy or negligence in publication in electronic or print media. Claims may be advanced under English law: ● Libel/slander – tort or Defamation Act 2013 ● Breach of copyright – contract or Copyright, Designs & Patents Act 1988 ● Trademark infringement – Trade Marks Act 1994
Regulatory Costs and Fines Cover	Regulatory Actions may arise in the UK as follows: ICO – in the context of cybersecurity regulatory action, this typically

	relates to breaches of the seventh data protection principle. There may also be industry specific regulatory actions, for example, the FCA is responsible for enforcing breaches of regulations applicable to financial services industries. Notable fines have been imposed for breach of PRIN 3 – the requirement to have adequate systems and controls.
Internal Investigation Cover	This bridges the gap before cover for regulatory fines and costs triggers (which typically covers "official, administrative or regulatory investigation or audit conducted by a Regulator"). With the growing focus by the regulators in the UK on informal early-cooperation investigations which are not "official", companies will often incur considerable expense in dealing with the matter before it reaches that point.
Payment Card Industry Data Security Standards (PCIDSS) Cover	Provides cover for the assessments of contractual fines by credit card brands for failure to comply with the Payment Card Industry Data Security Standards ("PCI DSS"). The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud. Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) or by a firm specific Internal Security Assessor that creates a Report on Compliance for organisations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes. The fines are contractual in nature as a contract has been entered into between the insured and the card provider and it is within that contract that the card provider and the insured have agreed to penalties for breaches in compliance Fines will be levied in all cases where merchants are the subject of a security breach and upon investigation are found to be non-compliant. Such fines include the costs of reissuance of affected credit cards and the reimbursement for fraudulent transactions to affected consumers. This coverage is becoming more important as it becomes evident that breaches affecting large amounts of consumer payment card information will result in mass reissuance of cards and substantial reimbursement of fraudulent transactions to the consumers by the card brands, which pass those costs back to the liable party.
Business Interruption Loss Cover	Whilst it is largely derived from property damage business interruption cover, and as such follows the same basic concepts, there are

	fundamental differences in the character of cyber losses and the interplay with policy wordings. Cyber business interruption claims are also potentially more complex and less tangible, and will often require different skills to quantify and adjust. Business interruption cover typically aims to indemnify loss of profit or revenue, as well as the increased cost of working and the costs of mitigating losses and getting back online. The trigger for cover is typically a security failure (a cyber-attack) however it is possible to extend coverage to a system failure (such as a degradation of the network from any cause) or human error which some businesses may find useful given that so many operations are online nowadays. Many policies require complete outage before business interruption kicks in. Others contain a trigger that means the suspension has to be actual and necessary. No company that suffers a slowdown in business because of a DDOS attack would want to be told that their cyber business interruption cover is worthless because they were never fully off line. Some policies limit cover to computer systems under the direct operational control of the insured whilst others extend cover to systems operated by third parties but still within the control of the insured. Policies nearly always include a waiting period before cover is triggered. Once triggered, losses incurred during the waiting period are recoverable. Time retentions in policies can vary from 6hr to 48hr depending on the risk and, of course, how much the policyholder wants to pay. The market norm is 10-hour time retention. The waiting period normally commences when the insured first discovers the BI event and notifies the insurer. Some policies only provide an indemnity for business interruption until the insured's computer system is fixed. Others provide for a longstop. Actual business interruption suffered by the insured following a cyber-attack can, in some circumstances, last beyond the time taken to repair its computer system.
Crisis Management Costs Cover	The costs a business may incur following a breach are numerous and a broad range of cover is available. Cover can include: ● Forensic Costs ● Data Breach Response Costs ● Data Identification and Preservation Costs ● Legal and Regulatory Advice Costs ● Notification costs ● Third Party Indemnification Advice Costs

	● Call Centre Costs ● Account and Credit Monitoring Costs ● Other Costs (to comply with any other legal requirement owed by the Insured to affected data subjects and Third Parties) ● Loss Adjustor Costs ● Reputation Advice Costs Reputational damage following a breach can be significant - cyber policies are generally not designed to cover such consequential loss.
Hacker Theft Cover	Covers the theft of money or securities by a computer e.g. hacking into payment system and diverting funds.
Cyber Extortion Cover	These kinds of attack are becoming more prevalent – the recent global WannaCry and Petya attacks demanded money for release of systems. Cyber extortion, including threats and/or ransom demands connected with cyber-attacks, is a risk which can cause great uncertainty for businesses - particularly in relation to how the extortion threat should be handled, for example, whether a ransom demand should be paid, whether such payment is legal and whether insurers may cover the ransom payments. This can be further complicated by the fact that the threat is often made with a short deadline for compliance with the demand. Demands are usually low in value e.g. the WannaCry demand was for $300. These relatively low sums tend to prompt businesses to pay the demand, particularly as it potentially results in the decryption and return of sensitive company information. There is no broadly applicable English legislation which makes ransom payments illegal. Additionally, there is also no general duty on ransom payers to report incidents to the police. There is also little legal commentary on the legality of ransom demands, cyber or otherwise. In the case of *Masefield AG v Amlin Corporate Member Ltd (The Bunga Melati Dua)* (a case relating to maritime piracy and ransom demands for safe return of the vessel and crew) the Court of Appeal held that there was no general public policy argument against paying ransoms and stated that: *"...there is no universal morality against the payment of ransom, the act not of the aggressor but of the victim of piratical threats, performed in order to save property and the liberty or life of hostages. There is no evidence before the court of such payments being illegal anywhere in the world. This is despite the realisation that the payment of ransom, whatever it might achieve in terms of the rescue of hostages and property, itself encourages the incidence of piracy for the purposes of exacting*

	more ransoms. (Perhaps it should be said that the pirates are not classified as terrorists. It may be that the position with regard to terrorists is different).” As the Court highlighted, ransom payments may be illegal in terrorism cases - Section 17 of the Terrorism Act 2000 (“TA00“) created an offence in respect of any person who enters into a funding arrangement and knows or reasonably suspects that it will or may be used for the purposes of terrorism. Therefore, if an insured knows or reasonably suspects that the cyber attackers are linked to terrorism, it could be an offence to pay the demand. Insurers cannot insure illegal acts so insureds and insurers should be mindful of this when considering whether to make a payment. Cyber extortion cover is usually subject to conditions, such as to keep the terms and conditions of the cyber extortion cover confidential, unless disclosure to law enforcement authorities is required; to take all reasonable steps to notify and cooperate with the appropriate law enforcement authorities; and to take all reasonable steps (including the involvement of a security consultant) to mitigate the loss.

We briefly set out here common features of/issues with cyber insurance.

- **Reasonable precautions clause:** Cyber policies typically include this clause, an example being: *"The Insured will take all reasonable measures (taking into account the size and complexity of the Insured and resources available) to safeguard the Company's Computer System and prevent the occurrence, and minimise the impact, of any Cyber Attack or Business Interruption Event."* The ever-evolving nature of cyber risks creates some challenges - what amounts to “reasonable precautions” in the context of cyber security? In the absence of a universal cyber security standard, this becomes a highly subjective question. It is therefore difficult to set a benchmark for minimum levels of cyber security for policy drafting purposes.

- **Betterment:** The issue of betterment is more likely to arise in relation to a cyber policy than, for example, a property policy. If an insured's computer network has suffered damage resulting from the exploitation of vulnerability, it would be inconceivable that the insured would repair the network to the pre-existing standard. However the extent of necessary repairs may be a source of disagreement between insurers and the insured.

- **Multiple insurance:** It is not uncommon for an attack to result in a data breach and business interruption e.g. cyber extortion often involves the threat to commit a data breach or business interruption. Accordingly, it is important to keep track of how retentions work, sub-limits, etc. as certain costs could potentially fall under multiple coverages.

- **Dishonest and misconduct exclusion:** Most conduct exclusions require "final adjudication" before they trigger. Depending on the wording, insurers may be able to rely on the exclusion where there has been a written admission of liability.

- **Trade secrets:** Cyber policies generally do not cover the value of the data to the insured. Therefore, if commercially sensitive data is released into the public domain, the financial consequences for the insured (which may be severe) are unlikely to be insured. Some cyber insurance policies, however, will offer coverage for infringement of intellectual property such as infringement of copyrights and trademarks, but not patent infringement or misappropriation of trade secrets.