Cybersecurity threats in the auto industry: Tensions in the knowledge environment

Morris, D., Madzudzo, G. & Garcia-Perez, A.

Original citation & hyperlink:
Morris, D, Madzudzo, G & Garcia-Perez, A 2020, 'Cybersecurity threats in the auto industry: Tensions in the knowledge environment', Technological Forecasting and Social Change, vol. 157, 120102.
https://dx.doi.org/10.1016/j.techfore.2020.120102

DOI 10.1016/j.techfore.2020.120102
ISSN 0040-1625

Publisher: Elsevier

Cybersecurity Threats in the Auto Industry: Tensions in the Knowledge Environment

David Morris*
Centre for Business in Society
Coventry University

Garikayi Madzudzo
Advanced Cyber Security Scientist
HORIBA MIRA, UK

Alexeis Garcia-Perez
Centre for Business in Society
Coventry University

***Corresponding Author**

d.morris@coventry.ac.uk
+44 797498 4023
Coventry Business School,
Coventry University,
Coventry CXV1 5FB
UK

Abstract

The automotive industry is undergoing probably the most far-reaching changes that have ever affected it. The outward manifestations of change are the emergence of the "connected" vehicle as the norm rather than the province of the up-market cars competing on the presence of innovative ICT-driven features, the race to develop fully autonomous vehicles (AVs) and the switch to more environmentally sustainable alternative fuel vehicles. The main enabler of these fundamental developments is technological change. But technology is also a driver of change, this is nowhere more obvious than in the application of ICTs in the transport arena. But technological changes of this magnitude also lead to changes in industry structure, a shift in the basis of competition from features and performance to functionalities, and a growing reliance on knowledge that is new to the traditional industry. This paper addresses one aspect of this milieu of developments, that is the emergence of cybersecurity threats to the modern highly-computerised vehicle. Countering such problems requires a high degree of knowledge sharing in the industry and particularly between car manufacturers and their supply networks. This article collects, synthesises and analyses some primary evidence from cybersecurity experts in the industry. The overall conclusion reached is that, in the view of auto-cybersecurity specialists, the level of knowledge-sharing is inadequate. The article presents a number of potential explanations for this phenomenon; the common feature of these explanations is the existence of significant tensions and lack of trust in the knowledge environment.

Key words: Cybersecurity**,** Knowledge-sharing**,** Auto industry**,** Supply networks**,** Trust

1. Introduction

The automotive industry is experiencing its greatest period of change since the introduction of mass production in the early part of the 20th. Century. The industry is simultaneously embracing the drive to create fully autonomous vehicles (AVs) and "connected" cars, a shift to more environmentally acceptable propulsion systems, including electric vehicles (EVs), and the much-anticipated change in culture from motoring based on private vehicle ownership towards mobility as a service (MaaS).

The term "connected vehicle" refers to one equipped with internet access, a wireless local area network, and built in capabilities that allow it to share digital information with other connected vehicles, physical devices, transport infrastructure, drivers and passengers. Increasing connectedness in cars is inter-twined with achieving higher levels of autonomy and ultimately a "driverless" car. The direction of causality in these developments is not important here, the cybersecurity consequences of increased dependence on, and exposure to, computer systems will be the same. Estimates of the likely number of connected vehicles abound, but one in five will have some sort of wireless connection by 2020, that is a quarter of a billion vehicles. The value of the 2021 connected vehicle market is estimated at €122bn (Allied Market Research 2018). The share of costs of electronics in the connected car value chain has risen from one-third now and is estimated to reach 50% by 2030 (Wagner 2019).

Industry estimates of the extent of computerisation in connected cars vary widely; but up to 150 embedded electronic control units (ECUs) and 300 million lines of code are no longer fanciful (Deichmann et al. 2019), making the vehicle highly dependent on numerous complex software systems and their seamless integration. Connected cars have become complex, pervasive and ubiquitous nodes on the Internet-of-Things (IoT). Whilst connected vehicles have the potential to deliver a wide range of benefits, particularly in the domain of safety and security, reducing harmful environmental impacts and extending the range of services available to users, these developments are not unambiguously beneficial. In particular, the greater the exposure of vehicles to digital environments, the greater related cybersecurity threats become. This tension between vastly more sophisticated vehicle performance and ever-increasing vulnerability to cybersecurity breaches has yet to be resolved at all relevant levels, including the car itself, road and associated infrastructure, and the auto industry in all its parts.

This paper argues that the effects of rapid development of vehicle connectivity and the expanding data environment connected cars inhabit, has led to tensions which need to be addressed. However, the paper does not discuss the major systemic tension inherent in the development of modern vehicles, that between the increased functionality and safety afforded by widespread computer connectivity and the raft of new opportunities for cybercrime which technological change creates. This theme is extensively explored elsewhere (see, for example, Kennedy et al. 2019). The roots of these tensions lie, in part, in the rapidly increasing complexity of automotive industry supply networks, the embodiment of unfamiliar technologies in industry products and the greater share of electronics in industry value chains. Furthermore, connected cars are only one element of a rapidly diversifying automobility ecosystem and expanding cybersecurity environment. Understanding the dynamics of the developing relationships between industry exploiters, managers and users of data on actual and potential cybersecurity threats, is a vital precursor to developing collective strategies for countering them. But possession of specialised cybersecurity knowledge also creates opportunities to gain competitive advantage by keeping it secret from competitors. Tensions arise when organisations simultaneously share their knowledge in alliances with others and, on the other hand, protect it to enhance individual performance (Bogers 2011).

The discourse and research on cybersecurity in the automotive industry has mainly concentrated on developing technical solutions and capabilities for the protection of assets, amelioration of organisational threats such as the need to protect core functions, and ensure business continuity, compliance with regulatory and legal policies and, to a much lesser extent, collaboration and cooperation strategies and processes (Craigen et al. 2014, Tisdale 2015). The theme of knowledge-sharing within the context of cybersecurity has remained in the relative shadows. The under-studied implications of growing cybersecurity threats for management and organisational structures, rather than technical issues per se, hold centre stage in this paper. As Pappas et al. (2018) demonstrate, the drive to design and implement sustainable and secure ways to profit from major changes in the data ecosystem presents major challenges for business leaders.

Figure 1 captures the main themes of this paper.

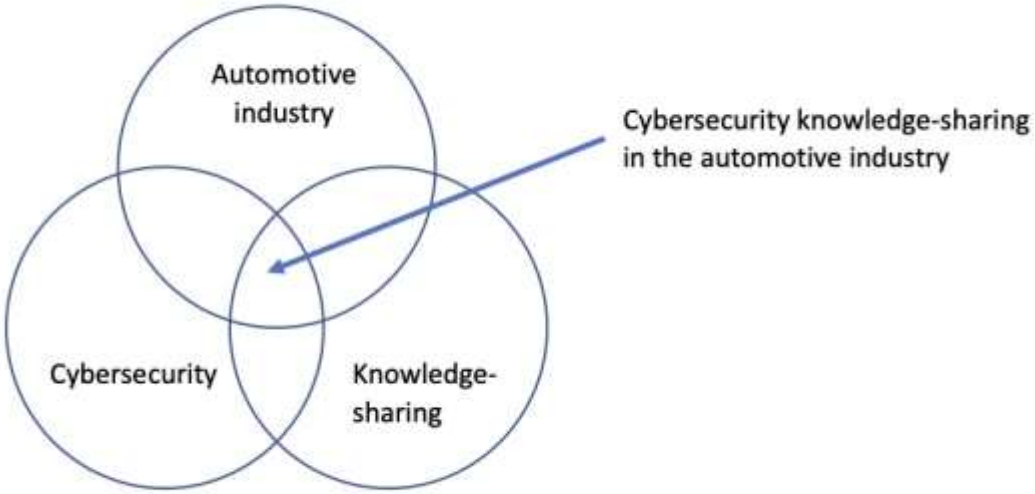

Figure 1. Major themes

2. Literature Review

The main question addressed by this paper is

How has auto industry responded to the cybersecurity knowledge management (KM) challenges posed by the development of ever more connected and autonomous vehicles?

2.1 The automotive industry

Modern vehicles have become pervasively connected. Internal connectivity is achieved through the use of electronic control units (ECUs) tasked with controlling and monitoring the internal vehicle network and its interconnected subsystems (Loukas 2015). Computer applications promote more informed manufacturing processes, the creation of new business models (Liu et al. 2012), reduced costs and risks (Leminen et al. 2012), enables real time data collection, and the integration of rapidly increasing numbers of software-based applications and improved product performance. The spread of the Internet of Things (IoT) in design, development and production processes has resulted in improved product performance (Aris et al. 2015), but also a greater reliance on design, engineering, production, and component out-sourcing which, in turn, is predicated on building trust with suppliers through greater knowledge-sharing.

2.2 Cybersecurity

Cybersecurity is a broadly used term, whose definitions are highly variable, context-bound, often subjective, and at times, uninformative. There is a substantial literature on what the term "cybersecurity" means and how it is situated within various contexts. Cybersecurity within a business or organisation is commonly protection focused on proprietary information, maintaining the integrity of databases, ensuring timely access to systems and information by authorised users, and preventing unauthorised access and damage to systems and their components. It aims to make an organisation more competitive and successful in a safe and secure environment. This involves strategies that enhance confidence with shareholders, customers and stakeholders, through to preventing damage to the business brand, actual losses and business disruptions.

In the context of this paper, cybersecurity is understood as:

the protection of vehicular electronic systems, communication networks, control algorithms, software, users, and underlying data from malicious attacks, damage, unauthorized access, or manipulation (NHTSA 2017).

Cybersecurity knowledge embraces both the component level and architectural knowledge used to protect connected vehicles, systems, sub-systems and embedded software. Component specific knowledge encapsulates the design concepts applied in component manufacturing processes; it includes design processes, component characteristics, manufacturing processes, security test results and functional and performance specifications which are applied within a specific component. Architectural knowledge includes architecture designs, design decisions, interface specifications, assumptions and parameters applied when integrating components into a system or sub-system.

Designing and developing cyber-resilient components and systems for connected vehicles is beyond the capabilities of a single supplier or OEM. Studies in automotive component manufacture highlight the importance of detailed component specific knowledge in ensuring secure component integration (Erdem et al. 2015). Cooperation between OEMs and their suppliers in the form of cybersecurity knowledge-sharing is a vital aspect of component design, development and integration.

Making vehicles is now based on integrating different components and technologies provided by a plethora of geographically dispersed suppliers. A component's functional and

performance parameters are important in understanding whether it will comply with the expected overall performance of the vehicle, while architectural knowledge is important in providing a holistic view; architectural knowledge embraces how components will be integrated into vehicle modules, systems or sub-systems and in identifying potential cyber-weaknesses in component manufacturing and integration processes.

2.3 Knowledge-sharing

Knowledge-creation and sharing influences organisational development and performance, and improves the ability of organisations to create solutions to problems. "Knowledge-sharing" embraces the ways in which knowledge may be shared between individuals, teams and organisations or combinations of them (Suppiah et al., 2011). It is important to understand where the boundaries of specific instances of knowledge-sharing lie; what knowledge is shared and with whom is a fundamental issue. The identification of "organisation" is particularly problematic; is it the individual firm, its supply network, R&D networks, the industry or some other grouping with common interests? Productive and valuable knowledge-sharing is built on three main pillars: voluntarism (Peng 2013), reciprocity and trust.

Knowledge sources are fundamental building blocks in promoting creativity and innovation in organizations. Knowledge-sharing helps develop new platforms for the development and introduction of new products and services (Wang and Noe 2010). Improved component design and integration strategies which cross supply chain networks can only be achieved through collaboration and collective effort rather than competition. Organisational knowledge is a corporate asset and needs to be managed as such, and, as a consequence, knowledge-sharing should be developed as a core organisational capability. There are clearly potential benefits to some specific aspects of knowledge sharing. For example, cyber threat intelligence (CTI) sharing can benefit all players in an industry by growing the collective stock of experience and thereby providing some protection to individual industry members from the possibility of reputation loss resulting from an unidentified threat and consequent cybersecurity breach (Wagner et al. 2019).

The automotive industry is, and has always been, a knowledge-sharing network (Schulze et al. 2015, Loebbecke et al. 2016, Kotabe et al. 2017); shared knowledge is an important resource underlying product development capability. Studies of the Japanese auto industry, particularly Toyota (Filippini and Forza 2016, Rinehart et al. 2018), and of the Chinese auto industry (Jean

et al. 2014, Corredoira and McDermott 2014, Khan et al., 2015) provide recent case evidence. Knowledge-sharing practices in the European automotive industry were highlighted by Schulze and Brojerdi (2014) and Loebbecke et al. (2016). However, the main concern of research to date has been new product development (NPD) (Blome et al. 2014;); much less attention has been paid to supplier and component integration (Yeniyurt et al. 2014).

This brief review suggests three broad industry developments which can potentially lead to tensions in the cybersecurity arena. The three areas are:

- The new technologies, greater complexity and changing roles at all stages in the value chain contingent on producing connected vehicles
- Greater use of component outsourcing, particularly in vehicle electronics
- Inadequately formulated and applied cyber-component integration strategies

These developments are not inclusive, others are also strong influences on the future direction of the industry. Nor are they exclusive to the automotive industry. There are lessons to be transferred between the auto industry and other domains, but this is a two-way process. The focus of this paper is firmly on the automotive industry and cybersecurity knowledge-sharing within it, but the challenges identified have clear resonance with those being encountered in other sectors. Whilst many industry players recognise the need to shift the balance of interactions away from protecting competitive advantage towards knowledge-sharing, one dimension of such change is that the search for improved cybersecurity creates tensions which are difficult to resolve.

3. Methodology

The empirical work which forms the major part of this study was based on an on-line survey of expert opinion. The survey results were themselves analysed and deepened via face-to-face semi-structured interviews with subject (automotive industry) cybersecurity experts. Using the two approaches provided elements of both methodological and data triangulation. However, the strength of the research in terms of its reliability, validity and credibility depends critically on the individual expertise of participants and their overall spread of knowledge in aggregate.
The participant sampling approach described here is purposive and seeks to cover a wide range of experience, knowledge and contexts without, on the other hand, losing focus on the specific

issues raised by cybersecurity knowledge-sharing. Participants in the study needed to meet the following ex-ante criteria:

- Be involved with connected vehicle development and manufacturing or connected vehicle component development and manufacturing
- Be involved in automotive cybersecurity issues and/or knowledge transfer processes in the automotive industry
- Their employer/organisation was involved in connected vehicle development research, and/or automotive cybersecurity research

3.1 Identification of potential participants

The identification of individuals who met these requirements and were willing to take part was a major practical issue. Four stages were adopted. Firstly, the researchers identified four global automotive companies, two OEMs and two major Tier 1 component suppliers, where contacts already known to the researchers through previous collaborative research were potentially readily available.

OEM 1 is a multinational automotive company with a focus on designing and building connected vehicles. Staff involved with cybersecurity issues, system and vehicle integration projects, automotive software engineering, in-vehicle security, automotive infotainment and telematics, and information security were potential participants.

OEM 2 has been involved in automated driving and intelligent driver assistance research since 2000. Employees from OEM 2 with skills and experience in in-vehicle security and diagnostics, automotive software design and development, component and software integration, and vehicle information security were candidates for participation in the study.

Supplier 1 manufactures connected automotive components prone to cyber-attacks such as ECUs, infotainment systems and vehicular telematics technology. Supplier 1 employs personnel with skill and experience in component integration, software integration, automotive software development and, software testing and validation.

Supplier 2 develops innovative solutions and expertise in connected mobility through its expertise in sensor technology, sensor software, and services. Supplier 2 services leading OEMs in connected vehicle and autonomous vehicle development.

At the second stage key contacts within these companies were approached to confirm their interest in the research and to suggest others within their organisation who satisfied the criteria identified for participants. This generated a starting list of potential participants which was then "cleaned" to reduce overlaps where appropriate and ensure a broad a range of expertise. At the third stage the research team provided this starting list of potential participants with information on the aims and objectives of the project, the researchers, ethical standards applied in the research including confidentiality, anonymity and security of data gathered, and the use which would be made of the results. The final (fourth) stage was the seeking of written confirmation that participants would be willing to take part. This stage was completed at the outset of interviews and as part of the distribution process for online questionnaires.

3.2 On-line questionnaires

The study makes use of online semi-structured questionnaires to gather data. The choice of online questionnaires was driven by the geographic nature of the automotive supply-chain, the complexity of the phenomenon being studied and the practical (logistical) problems of conducting face-to-face interactions.

The questionnaires asked about the participant's job role, title, duties and the length of time they had been employed in their current role. Open-ended questions explored how aware the participant and their organisation were of cybersecurity threats, the cybersecurity vulnerability mitigation measures being employed, the resources made available to promote automotive cybersecurity knowledge-sharing and any approaches in use. A final section contained a mix of closed and open-ended questions on component integration strategies employed by their own employer and supply chain partners. The online questionnaire was designed and distributed using the application Qualtrics.

Computer assisted qualitative data analysis (CAQDAS) was employed to code survey data collected via online questionnaires. CAQDAS enables the researcher to code and categorise collected data, as well as to organise and attribute meaning and relationships between codes (Gilbert et al. 2014, Silver & Lewins 2014). NVivo was used to code the survey data. NVivo is a powerful query tool that assists in organising and analysing non-numerical or unstructured data (Bazeley & Jackson 2013).

3.3 Face-to-face interviews

The data collected from the online questionnaires was supplemented by face-to-face interviews. The interviewing timetable ran alongside the online survey and interview data was not intended to be an input to the questionnaire design process or provide a means of deepening the online survey evidence by pursuing issues raised in questionnaires. This parallel approach can be characterised as qualitative interactionism with the aim of capturing evidence based on authentic experience (Silverman 2015).

The interviews lasted between 40-50 minutes and were all conducted at the interviewee's place of work. Interviews were audio recorded with consent and transcribed. Transcriptions were checked by the research team. Content analysis is dependent on creating codes or labels that can be applied in order to develop data into meaningful categories to be analysed and interpreted. There are two broad approaches to the coding of data: a priori coding where codes are created beforehand from existing theory (Corbin et al. 2014) and emergent coding where codes are drawn from participant generated evidence. Both approaches were used in the study.

Coding of the semi-structured face-to-face interview data was conducted manually rather than using a computerised coding process. Saldana (2015) supports manual coding in content analysis over computerised coding, arguing that it is more reliable and valid. Manual coding was also used given the relatively small number of cases and their diversity. Different terminology was used by different participants reflecting the global spread of the automotive industry and the ubiquity of cybersecurity challenges. One implication of this was that coding needed to be carried out by someone with their own expert knowledge of key cybersecurity issues. An initial list of potential a priori codes was developed inter alia from study of the sources identified in the literature review above. Emergent codes were a product of the iterations of the coding process itself.

3.4 Results

Data was collected during the period June to October 2018. Fifty-two experts from nine countries took part. Table 1 shows the distribution of participants by country and type of enterprise they belonged to.

Country	OEM-1	OEM-2	Supplier-1	Supplier-2	Total
Germany	3	2	2	1	**8**
India	0	0	3	0	**3**
Italy	2	1	2	1	**6**
Korea	1	0	0	0	**1**
Luxemburg	0	0	0	6	**6**
South Africa	2	0	0	0	**2**
Sweden	2	4	0	0	**6**
UK	4	5	2	3	**14**
USA	1	2	2	1	**6**
Totals	**15**	**14**	**11**	**12**	**52**

Table 1: Research participants by country and type of organisation

In overall terms the most surprising result is the lack of awareness of cybersecurity knowledge-sharing reported by participants. Participants were asked to state their level of awareness of cybersecurity knowledge-sharing initiatives involving their company. Table 2 provides the evidence.

Locus of cybersecurity knowledge-sharing	Aware	Not aware	Total
Between their OEM and other OEMs	11	18	29
Between departments in their OEM	18	11	29
Between OEMs and their supply networks	9	20	29
With their OEM customers	3	20	23
Between departments in their company	5	18	23
With their own suppliers	4	19	23

Table 2: Awareness of cybersecurity knowledge-sharing activity

The first three rows of the table summarise the combined responses of employees of OEM 1 and OEM 2. Rows 4-6 show the aggregated summary results for Supplier 1 and Supplier 2. Respondents' lack of awareness of cybersecurity knowledge-sharing initiatives and activities

reflects both absence of such activity and/or respondents' lack of knowledge of activities where they do exist. Disaggregating the results by employer (OEM 1, Supplier 1 etc) did not reveal any noteworthy differences.

Table 3 identifies the major issues identified by respondents. Figures in columns 2 and 3 are counts of the frequency with which each group stated an issue was a problem. For example, the first row of the table shows that asymmetry of relevant knowledge was mentioned 24 times by respondents from OEMs. By contrast the issue was not a major one according to suppliers. Figures are only shown if an issue count reached 10 or above across the 29 OEM respondents and eight for the 23 suppliers. Note that figures in cells do not equate to the total number of respondents in any category since an individual could identify as many or as few as they chose to. The figures shown are only indicative of relative importance of the different issues. In total OEM respondents identified twenty different issues, and suppliers fifteen.

Development	Frequency: OEMs	Frequency: Suppliers	Issue
Growing complexity of supply networks	24 18		Most of the relevant knowledge lies with suppliers. Component suppliers do not share component specific information. Information asymmetry between OEMs and suppliers.
Changing technologies of connected cars	16	 9 10	Skills shortages in cybersecurity issues. Obsolete software - components or architectures whose functionality is not fully understood. There is a resistance to change familiar manufacturing processes. Coding standards, different coding methods, styles and languages create cybersecurity challenges.
Competition	26 24 17	 19 17	Main goal is to manufacture and sell vehicles; sharing cybersecurity knowledge with competitors is a major challenge. Nature of competition creates a lack of trust between stakeholders. Incentives to share cybersecurity knowledge are weak or negative. Cybersecurity solutions need time and money to develop and implement; currently there is too little investment in knowledge-sharing. Emphasis on speed to market marginalises cybersecurity issues. There is a systemic underestimation of cybersecurity risks.
Increased reliance on outsourcing	21 12 16	 23 15 12 13	Component design being outsourced to reduce development times resulting in reduced knowledge-sharing. Growing use of NDAs and Design Contracts which restrict cybersecurity knowledge-sharing. Differences in legislation and regulatory requirements between countries can restrict knowledge-sharing. Differences in nationality, language, culture etc create different perspectives and approaches. Challenges of out-sourcing discourage cybersecurity knowledge-sharing.

Component integration	20	17	Over-reliance on suppliers for cyber-related solutions. Lack of a safe communication platform to discuss cybersecurity issues. Current strategies not designed to combat cybersecurity vulnerabilities.

Table 3: Major cyber-security knowledge-sharing issues identified by respondents

The evidence from the study emphasises a number of challenges that promote tension between the need for knowledge-sharing and the disincentives to revealing vulnerabilities and cybersecurity breaches. The nature and culture of competition in the industry is potentially the major hurdle to be overcome if cybersecurity knowledge-sharing is to play a significant positive role in the future development of AVs and connected cars. As a cybersecurity expert from a major systems integrator/supplier put the case:

When it comes to cybersecurity knowledge-sharing, there is none ……because every player is trying to protect themselves in order to make sure that they will introduce into the market that trend or that highly innovative product before their competitors and at the end of the day everyone is trying to make money. (Cybersecurity expert, Supplier 2).

OEMs and component suppliers compete both in maximising market share and innovation leadership. This creates an environment whereby cybersecurity and the sharing of cybersecurity-related information, practices and approaches are viewed as an obstacle that affects sales and hinders innovation. A senior manager from OEM 1 emphasised the role of speed to market as a competitive force:

Cybersecurity sort of creates more problems in delays in getting the vehicles out there, and the senior managers, at the top are not interested in problems, they want to get vehicles out to market. Sell one million vehicles a year that's all we interested in, anything else we will sort it out after. If an engineer identifies a flaw, and approaches management, they will be okay we will fix it, that's a flaw, we will fix that, we will look into that. It then gets elevated up to pounds and dollars, then it's yeah we're not doing that. (Senior manager, OEM 1).

The head of one of the major divisions at Supplier 2 underlined the issue:

Due to the competitive nature of the industry, it's a race to see who is going to bring the next innovative product to market, I remember the first man on the moon, l don't know who the

second was, so we are in a very competitive industry, a very fast moving industry, and the only way to try and stay ahead is to keep your cards close to your chest. (Senior manager, Supplier 2).

The lack of trust is also a feature of relationships between suppliers. This is reflected in the increased use of non-disclosure agreements (NDA's), and design contract agreements. A cybersecurity engineer from a systems integrator stated:

There is no trust been us as suppliers, to the point that when we have meetings during a joint collaboration, the meetings are heavily restricted to the point where it is almost useless, no one wants to share anything that they think will give them an edge over the other suppliers. (Cybersecurity engineer, Supplier 2).

The attitude towards cybersecurity protection in the automotive industry is that it delays production, increases development costs and does not increase the overall value of the product. "Value" is here being interpreted as the monetary value as measured by the market price of the car. Not only is it difficult to measure or explain cybersecurity and its benefits to customers it is also not normally possible to put a price on them or measure consumers' willingness to pay for cybersecurity features. This has in turn created an environment whereby cybersecurity is viewed as less important compared to saleable features and, to a lesser extent, safety. This was noted by a head of cybersecurity:

Because they have to get the vehicles out to market quick, and they have to compete with all their competitors and stuff like that, it has built a situation where security is taking a side door. It has taken fifteen years for the UK vehicle industry to consider safety properly. There is more of a safety culture now than there was, but there is no security culture. (Cybersecurity Lead, Supplier 2).

Lack of trust and the highly competitive nature of the industry were not the only factors highlighted as sources of tension between the need for knowledge-sharing as a pre-requisite for effective action and the disincentives to reveal vulnerabilities and cybersecurity breaches. Participants argued that lack of knowledge and appropriately skilled personnel has resulted in a dearth of mechanisms to encourage and promote cybersecurity knowledge-sharing at all levels within and across the automotive spectrum. As a consequence, some OEMs have become over-reliant on component manufacturers to provide cybersecurity solutions and applications. Component suppliers, in a bid to remain relevant, have capitalised on this gap by retaining and guarding the relevant knowledge; a head of research at a major component supplier stated:

When we talk to OEMs, from the questions they ask, you can tell they do not know, they do not have the information if l may say. They need to go and get the knowledge so that they can ask the right questions. They need to find some time and resources to go and find details of each component to be able to discuss at the same technical level as us. (Head of Research, Supplier 2).

The tensions result from asymmetry of knowledge present were expressed by an OEM vehicle component integration manager:

There is not a lot of sharing between vehicle manufacturers and component manufacturers because most OEMs do not have the technical knowledge. Suppliers have the knowledge, but they really don't want to share the knowledge, I mean they just want OEMs to sign the contract, win their confidence and tell them that everything is fine. Some Germany suppliers are starting to be a little bit flexible, which is a good thing but the information they provide is very much limited to be useful. (Integration manager, OEM 2).

The over-reliance on component suppliers by OEMs in the design and development of technology has created an environment whereby most of the knowledge resides with component suppliers and informed co-creation and debate between them is lacking. A senior manager from a major supplier pointed out the dangers to OEMs of knowledge asymmetry:

The transfer of knowledge is too oriented around the suppliers and not so by the vehicle manufacturers. OEMs are too reliant on suppliers, for example OEM X are too reliant on component supplier Y. So, in the event that component supplier Y develops a component for OEM X that is not of high quality, OEM X are not big enough to go back to component supplier Y and dictate to them and say this is what we need, and these are the requirements, no. Company supplier X, will provide OEM X with a pre-defined solution because they (OEM X) cannot provide the information themselves. They are then forced to re-factor their architecture to accommodate the solution in, basically they might be creating holes in their security architecture by doing so. So basically, they get what they are given. (Senior manager, Supplier 1).

Software creates particular issues. A director of a major systems integrator explained:

A component supplier might provide an OEM with a component, but they will not tell the OEM how they have designed and manufactured the component. It might seem like that is good for business, but it is really not a good situation from my perspective because l am thinking, well

there is software in there, for example the OEM knows it is there but they do not know anything about what it does, there is no understanding on what it does, which again is a threat according to threat analysis. (Research Director, Supplier 2).

4. Discussion and implications

The literature review identified three broad and interlinked trends which create tensions in the automotive cybersecurity domain. New forms of industry players are exerting a strong influence on the ability of the industry as a whole to anticipate, identify, counter and manage cybersecurity threats. These threats are not simply the product of crimanl and other mal-intentioned activity, but are a product the changing structure of supply networks, including the rise of systems and integrators. Some of these roles have been taken on by existing Tier 1 suppliers, others by major organisations with their roots in other domains, for example ICT companies, and yet others by new entrants. Of course, OEMs retain overall responsibility for the integrity of their products, including safety and security. This raises a number of questions as the evidence gathered from industry experts, summarised in Table 3, shows.

According to the study's participants, current component integration strategies are not designed to address cybersecurity vulnerabilities. When the few participants who demonstrated an awareness of integration strategies used by their organisations were asked whether those strategies addressed or provided relevant information and steps to cater for cybersecurity threats, they reported that those currently in use were designed and developed before the introduction and inclusion of the electronic control systems and software modules deployed in modern connected vehicles. Current integration strategies were developed before the ubiquitous implications of automotive cybersecurity threats were appreciated and, as a result, most component integration strategies are not cyber-resilient.

The results in Table 3 also reveal an over-reliance by OEMs on suppliers to design and develop technical and technological solutions to automotive cybersecurity threats. This limited or constrained participation by OEMs in cyber-vulnerable component design and integration processes, coupled with NDAs and contractual agreements, has culminated in component suppliers being the gate-keepers of much of the cyber-related knowledge. This over-reliance on component suppliers is validated by the extremely low numbers of personnel employed in their OEMs' cybersecurity departments. One major UK-based OEM only has a team of two individuals who have been recently recruited to manage their cybersecurity affairs, however there are plans to increase the team to forty. This low level of specialists was repeated in other

OEMs. By contrast two of the major systems integrators had much higher levels of specialist input. The UK arm of one major European supplier employed twenty cybersecurity experts with at least 20-30 years of experience between them. At the other end of the scale, one global player currently employs 128 automotive cybersecurity experts, with an additional 19,000 personnel worldwide covering various automotive cybersecurity related work such as regulation and legislation of connected vehicles.

In the view major suppliers, most OEMs do not have sufficient technical or specific knowledge of the cyber-vulnerable components they integrate into their product architectures. This lack of cybersecurity knowledge is one of the reasons why OEMs may ignore secure development practices in the design and development of connected vehicles. Additionally, some of the software code that exists in connected vehicles is obsolete, written in old software language versions that most current automotive system integrators are not familiar with; they are unable to determine its functionality or relevance. In addition, they may be unable to predict potential consequences if it were removed.

The automotive industry has conventionally relied on, and encouraged knowledge-sharing. Prior to the introduction of electromechanical constructs in vehicles, OEMs relied on knowledge-sharing as a key element in developing and maintaining high involvement relationships with suppliers. Studies of the European, Chinese and Japanese auto industry provide evidence of the existence of knowledge-sharing practices and their major role in improving vehicle manufacturing. However, the introduction of technologies that permit vehicles to connect to and communicate with and across their internal and external environments has impacted on the automotive supply chain. A new breed of entrants has pushed vehicle manufacturers away from their traditional core technology base and rendered familiar knowledge-sharing approaches outdated. In particular, traditional knowledge-sharing mechanisms based on a tiered supply chain model have struggled to counter cybersecurity issues. As Bryans (2017) notes, the lack of economic incentives to share knowledge, and the lack of effectiveness of the information being shared, have promoted a lack of participation.

Manufacturer intrusiveness reflects the level of detail an OEM employs in defining the design of an artefact. The level of intrusiveness influences the cybersecurity knowledge the OEM has about the component and leads to insights on how cybersecurity vulnerabilities may arise and what mitigation measures may be required to address any cybersecurity threat. However, globally dispersed component suppliers jealously guard cybersecurity knowledge despite

often having limited access to details of the vehicle architecture where their components will reside.

A lack of trust between OEMs, between suppliers and between OEMs and suppliers is also evident. This lack of trust has seen the spread of Non-Disclosure Agreements (NDAs), Design Contracts and Confidentiality Agreement Contracts in joint projects and third-party contractors. This can be attributed to a number of factors, such as the competitive nature of the industry and the perceived need to protect Intellectual Property (IP) including design documents. The potential costs to OEMs of loss of reputation contingent on cybersecurity failings is also relevant and compounded by their lack of technical knowledge in regard to the components or cyber-solutions that they integrate into their products. In addition, top managers may view cybersecurity as a design requirement that delays vehicles to market, an after-thought that delays production and increases development costs. The automotive domain is far from static. Standards and practices are developing rapidly and the push towards more open models, institutions and behaviours is gathering pace. Hopefully these will enhance trust rather than hinder much needed change.

Our study has, of course, major limitations. In particular a larger number of face-to-face interviews would have provided greater insight into the origin and consequences of cybersecurity knowledge gaps. However, detailed studies which focus on gathering qualitative data are, at best, rare. Previous research on the automotive industry has focused attention on the role of knowledge-sharing in new product development (NPD) (Lawson et al. 2015, Tuli and Shankar 2015) and little emphasis has been placed on component integration (Yeniyurt et al. 2014); this is an important gap to fill.

References

Allied Market Research, Global Opportunity Analysis and Industry Forecast, 2018 – 2025, Connected Car Market Value by Technology: Global Opportunity Analysis and Industry Forecast, 2018 - 2025 [online] available from: <https://www.alliedmarketresearch.com/connected-car-market> [March 2018].

M Amin, Z Tariq, Securing the Car: How Intrusive Manufacturer-Supplier Approaches Can Reduce Cybersecurity Vulnerabilities. Technology Innovation Management Review 5 (1), (2015), p.21.

I B Aris, R K Z Sahbusdin, A F M. Amin, Impacts of IoT and Big Data to Automotive Industry, Control Conference (ASCC), 2015 10th Asian.: IEEE

P Bazely, K Jackson, Qualitative Analysis with NVivo, (2013) Sage Publications

C Blome, T Schoenherr, D Eckstein, The Impact of Knowledge Transfer and Complexity on Supply Chain Flexibility: A Knowledge-Based View. International Journal of Production Economics 147, (2014) 307-316

M Bogers, The open innovation paradox: knowledge sharing and protection in R&D collaborations, European Journal of Innovation Management, 14(1) (2011) 93-117.

S Brown, J Gommers, J O Serrano, From Cyber Security Information Sharing to Threat Management, Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security. (2015) ACM.

J Bryans, The Internet of Automotive Things: Vulnerabilities, Risks and Policy Implications. Journal of Cyber Policy 2 (2), (2017) 185-194.

A Cabigiosu, F Zirpoli, A Camuffo, Modularity, Interfaces Definition and the Integration of External Sources of Innovation in the Automotive Industry, Research Policy 42 (3), (2013) 662-675.

R Corredoira, G McDermott, Adaptation, Bridging and Firm Upgrading: How Non-Market Institutions and MNCs Facilitate Knowledge Recombination in Emerging Markets. Journal of International Business Studies 45 (6), (2014) 699-722.

D Craigen, N Diakun-Thibault, R. Purse, Defining Cybersecurity, Technology Innovation Management Review 4 (10): (2014)13-21.

J Deichmann, B Klein, G Scherf, R Stützle, The race for cybersecurity: Protecting the connected car in the era of new regulation, McKinsey Center for Future Mobility, October 2019.

J Ďurišová, Knowledge Life Cycle and its Application in Automotive Industry. Problems of Management in the 21st Century 2, (2011) 45-53.

I Erdem, H Kihlman, A Andersson, Development of Affordable Reconfigurable Tooling in Car Manufacturing Cells–A Case Study, 23rd International Conference for Production Research, ICPR 2015, Manila, Philippines, 2015, 2-6 August

R Filippini, C Forza, The Impact of the Just-in-Time Approach on Production System Performance: A Survey of Italian Industry. A Review and Outlook. in A Journey through Manufacturing and Supply Chain Strategy Research. ed. by Anon: Springer, (2016) 19-39.

P Fraga-Lamas, T Fernandez-Carames, A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry. IEEE Access, 7, (2019). 17578-17598.

L S Gilbert, K Jackson, S di Gregorio. Tools for Analyzing Qualitative Data: The History and Relevance of Qualitative Data Analysis Software, IN Handbook of Research on Educational Communications and Technology. Springer (2014) 221-236

K Goffin, U Koners, (2011) Tacit Knowledge, Lessons Learnt, and New Product Development. Journal of Product Innovation Management 28 (2), (2011) 300-318.

Y He, N. Zhao, N H. Yin, (2018) Integrated Networking, Caching, and Computing for Connected Vehicles: A Deep Reinforcement Learning Approach, 67 (1), (2018) 44-55.

R Jean, R Sinkovics, T P Hiebaum, The Effects of Supplier Involvement and Knowledge Protection on Product Innovation in Customer–Supplier Relationships: A Study of Global Automotive Suppliers in China. Journal of Product Innovation Management 31 (1), (2014) 98-113.

J Kennedy, T Holt, B Cheng, Automotive cybersecurity: assessing a new platform for cybercrime and malicious hacking. Journal of Crime and Justice 42 (5), (2019) 632-645.

Z Khan, O. Shenkar, Y Lew, Knowledge Transfer from International Joint Ventures to Local Suppliers in a Developing Economy'. Journal of International Business Studies 46 (6), (2015) 656-675.

M Kotabe, C Jiang, J Murray, Examining the Complementary Effect of Political Networking Capability with Absorptive Capacity on the Innovative Performance of Emerging-Market Firm, Journal of Management 43 (4), (2017)1131-1156.

B Lawson, D Krause, A Potter, Improving Supplier New Product Development Performance: The Role of Supplier Development. Journal of Product Innovation Management 32 (5), (2015) 777-792.

S Leminen, M Westerlund, M Rajahonka, R Siuruainen, (2012) Towards IOT Ecosystems and Business Models. in Internet of Things, Smart Spaces, and Next Generation Networking. Springer, (2012) 15-26.

T Liu, R Yuan, H Chang, Research on the Internet of Things in the Automotive Industry. 2012 International Conference on Management of e-Commerce and e-Government IEEE, (2012), 230-233

C Loebbecke, P van Fenema, P Powell, Managing Inter-Organizational Knowledge Sharing. The Journal of Strategic Information Systems 25 (1), (2016) 4-14.

G Loukas, Cyber Physical Attacks on Implants and Vehicles, in CYBER-PHYSICAL ATTACKS: A Growing Invisible Threat. Oxford, England: Elsevier, (2015) 82-102.

A Manello, G Calabrese, The influence of reputation on supplier selection: An empirical study of the European automotive industry, Journal of Purchasing and Supply Management, *25*(1), (2019), 69-77.

D Morris, G Madzudzo, A Garcia-Perez, Cybersecurity and the Auto Industry: The Growing Challenges Presented by Connected Cars. International Journal of Automotive Technology and Management 18 (2), (2018) 105-118.

NHTSA, Cybersecurity Best Practices for Modern Vehicles [online] available from <https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/sae2017chatipoglu_0.pdf> [June 2017].

I Pappas, P Mikalef, M Giannakos, J Krogstie, G Lekakos, Big data and business analytics ecosystems: paving the way towards digital transformation and sustainable societies, Information Systems and e-Business Management, 16 (3) (2018) 479-491

H Peng, Why and When do People Hide Knowledge? Journal of Knowledge Management 17 (3), (2013) 398-415.

J Rinehart, J Huxley, D Robertson, Just another Car Factory: Lean Production and its Discontents.: Cornell University Press., 2018

J Saldana The Coding Manual for Qualitative Researchers, (2015) Sage Publications

A Schulze, G Brojerdi, G von Krogh, Those Who Know, do. those Who Understand, Teach. Disseminative Capability and Knowledge Transfer in the Automotive Industry'. Journal of Product Innovation Management 31 (1), (2014) 79-97.

A Schulze, P MacDuffie, F Täube, Introduction: Knowledge Generation and Innovation Diffusion in the Global Automotive Industry Change and Stability during Turbulent Times. Industrial and Corporate Change 24 (3), (2015) 603-611.

C Silver, A Lewins, Using Software in Qualitative Research: A step-by-Step Guide, (2014) Sage Publications

V Suppiah, M Singh Sandhu, Organisational Culture's Influence on Tacit Knowledge-Sharing Behaviour, Journal of Knowledge Management 15 (3), (2011) 462-477.

R Trope, T Smedinghoff, Why Smart Car Safety Depends on Cybersecurity, *Scitech Lawyer* 14 (4), (2018) 8-13.

D Teece, Nonaka's Contribution to the Understanding of Knowledge Creation, Codification and Capture. in Towards Organizational Knowledge. ed. by Anon: Springer, (2013) 17-23.

S M Tisdale, Cybersecurity: Challenges from a Systems, Complexity, Knowledge Management and Business Intelligence Perspective. Issues in Information Systems. 16 (III) (2015) 191-198

P Tuli, R Shankar, Collaborative and Lean New Product Development Approach: A Case Study in the Automotive Product Design. International Journal of Production Research 53 (8), (2015) 2457-2471.

T Wagner, K Mahbub, E Palomar, A Abdallah, Cyber threat intelligence sharing: Survey and research directions, Computers & Security, (2019) 87, 2019

I Wagner, Automotive electronics cost as a share of total car cost 1950-2050. 23 October 2019. Available at:

https://www.statista.com/statistics/277931/automotive-electronics-cost-as-a-share-of-total-car-cost-worldwide/

S Wang, R Noe, Knowledge Sharing: A Review and Directions for Future Research, Human Resource Management Review 20 (2), (2010) 115-131

S Yeniyurt, J Henke, G Yalcinkay, A Longitudinal Analysis of Supplier Involvement in Buyers' New Product Development: Working Relations, Inter-Dependence, Co-Innovation, and Performance Outcome, Journal of the Academy of Marketing Science 42 (3), (2014) 291-308.