



Cybersecurity for Connected and Autonomous Vehicles

Considerations and opportunities for growth

September 2019

Executive Summary

Background

Connected and autonomous vehicles (CAVs) are captivating consumers, industry and governments around the world. Although CAVs are designed with capabilities and features that have the potential to provide increased safety, satisfaction, comfort and convenience, CAVs also bring emerging challenges to security and privacy – with a combination of physical and digital threats.

The Cybersecurity for Connected and Autonomous Vehicles: Considerations and Opportunities for Growth report was commissioned by the Autonomous Vehicle Innovation Network (AVIN) and the Automotive Parts Manufacturers' Association (APMA) to give a high-level overview of the CAV cybersecurity threat landscape, and to highlight both the opportunities and risks associated with emerging CAV technologies with a focus on strategies, standards, solutions and market opportunities for Ontario.

Objective and Methodology

In the context of growing cybersecurity threats, and with concerns about safety, security, efficiency and data privacy, this report's aim is to identify key areas for consideration and avenues for growth and development. While Ontario's CAV market is increasingly dealing with challenges, it is also identifying and capitalizing on opportunities to increase our understanding of CAV cybersecurity threats, and continuing to innovate in this space to become a global market leader.

Using a layered approach of secondary and primary research, this report summarizes insights across a complex CAV ecosystem. Primary research methods included a survey and a series of interviews and validation discussions with key stakeholders and subject matter experts from Ontario and other leading jurisdictions.

Considerations and Opportunities

Our global research and CAV stakeholder responses highlighted that authentication and trust will be key challenges across the CAV ecosystem and that the entire extended security perimeter must be considered, with a focus on cloud security, in-vehicle security, and network security. Considerations around standardization, collaboration, training and trust add complexity to being able to respond to and manage CAV cybersecurity risks.

Stakeholders across the CAV landscape globally are identifying cybersecurity as a critical component to ensuring the safety and security of the future of mobility, and have identified opportunities to collaborate across government and industry. These opportunities include:

- | | |
|--|--|
|  Standardization, certification and legislation |  Bringing OEM and technology innovation to market |
|  Skilled talent growth and retention |  Convergence security testing |
|  Collaboration and partnerships across industries |  Privacy and security by design; ethical frameworks |
|  Trust and authentication innovation | |

Ontario CAV cybersecurity stakeholders are telling us there is still a way to go in terms of clarity on requirements, partnerships, and support for CAV cybersecurity – but there are a lot of opportunities to continue to establish Ontario as the go-to market for this core component to the success and adoption of CAVs around the world.

About Us

AVIN is an initiative by the Government of Ontario that is delivered by the Ontario Centres of Excellence (OCE). AVIN is ensuring that Ontario captures the economic opportunity presented by CAV technology and mobility solutions to create jobs in our province, while ensuring that Ontario leads in readiness, adoption and deployment. AVIN supports the development and demonstration of CAV technologies including infrastructure technologies, commercially ready technologies for application in light and heavy-duty vehicles (including cars, commercial vehicles, trucks, buses, and recreational vehicles), intelligent transportation systems (ITS), and transit-supportive technologies.

APMA have partnered with AVIN to operate the AVIN Technology Demonstration Zone located in Stratford, Ontario. The APMA is Canada's national association representing OEM producers of parts, equipment, tools, supplies, advanced technology, and services for the worldwide automotive industry. The Association was founded in 1952 and its members account for 90% of independent parts production in Canada. In 2018, automotive parts shipments were over \$35 Billion and the industry employment level was over 100,000 people.

Deloitte's Future of Mobility practice serves the entire ecosystem of companies working in and around mobility. The entire way we travel from point A to point B is changing, and this transformation is creating a new ecosystem of personal mobility, with implications affecting more than just the automotive industry. Deloitte's Cyber Risk services help organizations solve complex problems and perform better, so they can build confident futures – futures that are better for business, better for people, and better for the planet. Using human insight, technological innovation, and comprehensive cyber solutions, Deloitte manages cyber everywhere so society can go anywhere.

Contents

● Introduction and methodology	3
● Autonomous vehicles and the future of mobility	6
● Global CAV testing and pilot legislation and standards	7
● Ontario's CAV innovation ecosystem and stakeholder landscape	8
● CAV cybersecurity threat landscape	10
● Global cybersecurity developments in the CAV landscape: Strategies, legislation, and industry driven standards and regulations	14
● Solution developments in the CAV landscape and innovation models	17
● CAV cybersecurity considerations: Top stakeholder themes	19
● Key global considerations for CAV cybersecurity	20
● Key opportunities for CAV cybersecurity in Ontario	21
● Conclusion	22
● Endnotes and key terms	23
● Appendix	27

Introduction



Introduction

Connected and autonomous vehicles (CAVs) are captivating consumers, industry and governments around the world. Although CAVs are designed with capabilities and features that have the potential to provide increased safety, satisfaction, comfort and convenience, CAVs also bring emerging challenges to security and privacy – with a combination of physical and digital threats.

The connected and autonomous vehicle defined

Transport Canada defines connected vehicles as “vehicles using different types of wireless communication technologies to communicate with their surroundings”.¹ An autonomous or automated vehicle is described as using a “combination of sensors, controllers and onboard computers, along with sophisticated software, allowing the vehicle to control at least some driving functions, instead of a human driver”. As we move towards increasingly connected and more autonomous vehicles, the complexity of managing threats to those vehicles – and their passengers – also increases.

The benefits and risks of vehicle connectivity and automation

Safety is a paramount driving force for automation, particularly given the fact that the vast majority of the serious crashes are due to human error. CAVs have the potential to reduce injuries and save lives. CAVs can increase the efficiency of mobility by decreasing traffic congestion and can deliver economic benefits by increasing productivity and providing new avenues for mobility options. Similar to how laptops and mobile phones have augmented human capabilities, CAVs strive to create a more enabled, engaged and integrated driver experience and ecosystem.

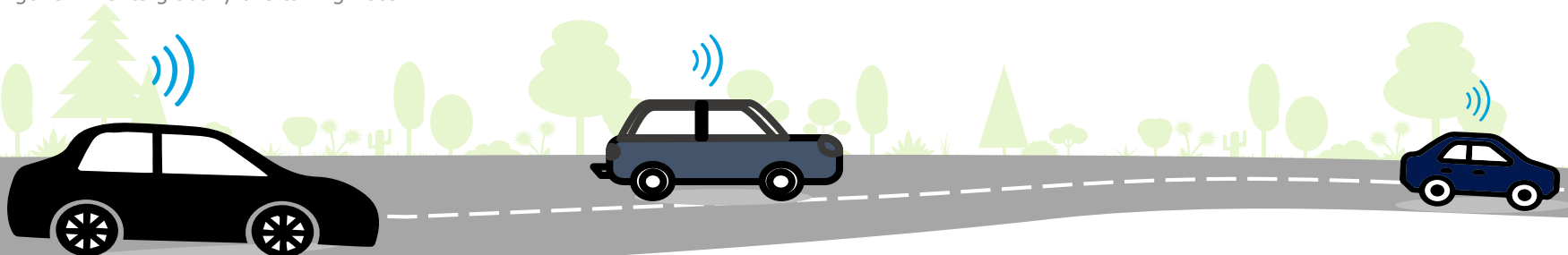
The CAV ecosystem is growing and spans from infrastructure, to vehicle manufacturers, to service providers, to customers. Risks and impacts are increasing along with consumer demand for availability, and industry and governments globally are taking note.

In Canada, there have been a number of recent reports highlighting cybersecurity’s impact on CAVs.² The Standing Senate Committee on Transport and Communications released a report in 2018 titled “Driving Change: Technology and the future of the automated vehicle”, which highlighted significant security and privacy concerns. This year, Transport Canada released a safety assessment tool that considers cybersecurity. The Policy and Planning Support Committee (PPSC) Working Group on Automated and Connected Vehicles developed a policy framework for CAVs that recommends public awareness of cybersecurity vulnerabilities. Innovation, Science, and Economic Development Canada (ISED) publicly stated that they will be supporting an amendment to the *Personal Information Protection and Electronic Documents Act (PIPEDA)* to enhance the enforceability of privacy legislation. ISED further emphasized the emergence of autonomous vehicles as an important reason for revamped privacy mechanisms in the 2019 Digital Charter announcement.²

In the context of major cyber incidents impacting vehicles globally, the 2019 World Economic Forum (WEF) Global Risks Report³ highlighted a key trend with large impacts to the CAV ecosystem:

A rising cyber dependency due to the increasing digital interconnection of people, things, and organizations, with potential impacts on key infrastructure and investment.

Ontario’s CAV market is increasingly dealing with these considerations, but is also seeing interesting opportunities to increase our understanding of CAV cybersecurity and innovate in this space to become a market leader globally.

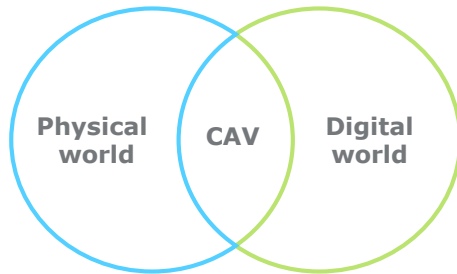


Methodology



The Need for a CAV Cybersecurity Framework

Cybersecurity risks are particularly complex for CAVs, as they operate across both the physical and digital world, and both consume and create data, while communicating with the surrounding ecosystem.



Risks to CAVs involve threats related to:

- The vehicle,
- The CAV ecosystem, and
- The data collected.

According to the National Institute of Standards and Technology (NIST), risk mitigation for complex Internet of Things (IoT) devices needs to look at protecting device security, data security, and individuals' privacy⁴ – which is precisely the case for CAVs. This complex CAV ecosystem requires a framework that considers Security Convergence (the combination of physical security and cybersecurity) and the concept of Privacy by Design.

The Deloitte Cyber Strategy Framework (CSF), supported by our Privacy by Design framework and Security Convergence methodology, allows for the analysis of key capabilities needed to mitigate emerging threats to CAVs. The Deloitte CSF covers the need for cybersecurity **governance**, along with **secure**, **vigilant**, and **resilient** capabilities.

The application of any cybersecurity framework to the CAV environment must consider the full ecosystem and each stakeholder to understand the range of risks and opportunities.

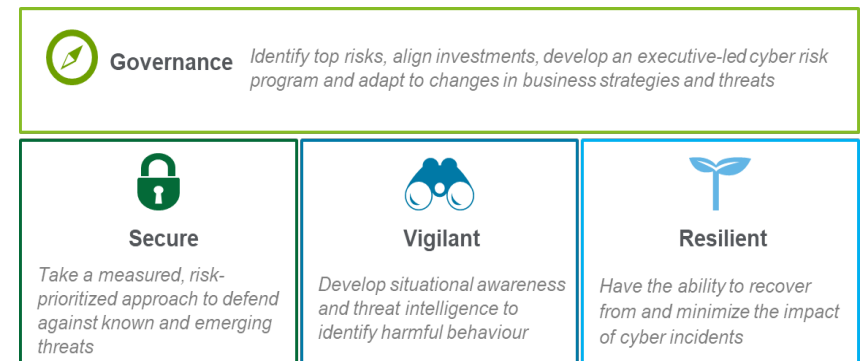
See the Appendix for more details on the Security Convergence and Privacy by Design frameworks.

Objective and methodology

The Autonomous Vehicle Innovation Network (AVIN) is an initiative by the Government of Ontario that is delivered by the Ontario Centres of Excellence (OCE). AVIN is ensuring that Ontario captures the economic opportunity presented by CAV technology and mobility solutions to create jobs in our province, while ensuring that Ontario leads in readiness, adoption and deployment. AVIN supports the development and demonstration of CAV technologies including infrastructure technologies, commercially ready technologies for application in light and heavy duty vehicles (including cars, commercial vehicles, trucks, buses, and recreational vehicles), intelligent transportation systems (ITS), and transit-supportive technologies.

In the context of growing cybersecurity threats, concerns about vehicle data collection, as well as CAV opportunities in Ontario, this report's aim is to identify key areas for consideration and avenues for growth and development. Using a layered approach of secondary and primary research, this report summarizes insights across a complex CAV ecosystem. Primary research methods included a survey and a series of interviews and validation discussions with key stakeholders and subject matter experts from Ontario and other leading jurisdictions.

The four pillars of Deloitte's CSF



More on the connected and autonomous vehicle

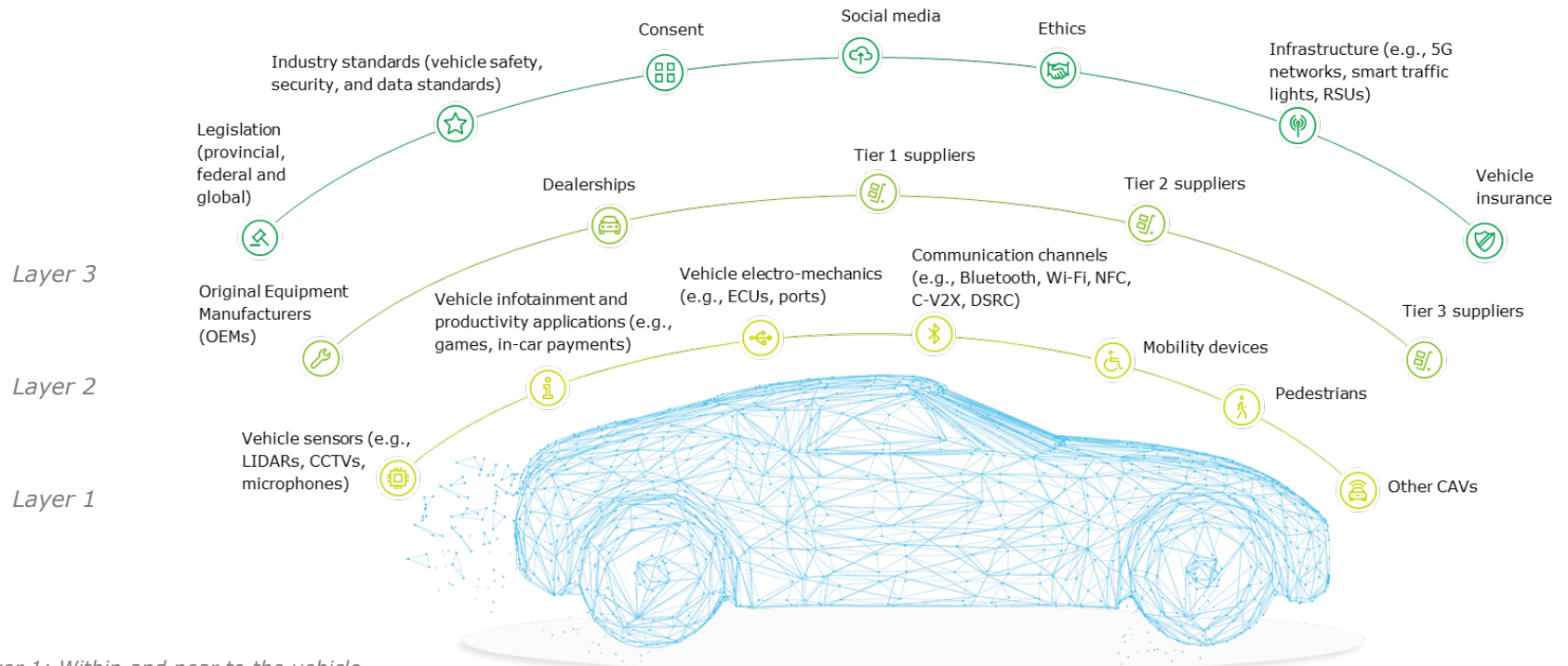


CAV connectivity, features and attributes

The connected and autonomous vehicle can be referred to as a combination of various IoT devices with the capability to communicate with its surrounding physical and digital environment. Depending on the features installed, a connected vehicle may be able to communicate with the following:

- Its occupants, other vehicles (vehicle-to-vehicle or V2V), other connected devices (e.g., mobile phones), and road users
- Internet-based applications
- A Security Credential Management System (SCMS)
- The surrounding transportation physical infrastructure such as traffic signal controller, roadside units (RSUs) and digital infrastructure such as communication networks and cloud systems – collectively called as vehicle-to-infrastructure or V2I

The image below provides examples of attributes associated with a CAV – from connectivity inside or close to the vehicle, to key third parties, to the surrounding environment and considerations.



Layer 1: Within and near to the vehicle

Layer 2: Supply chain

Layer 3: Extended ecosystem and relevant considerations

Autonomous vehicles and the future of mobility

Moving towards autonomous vehicles

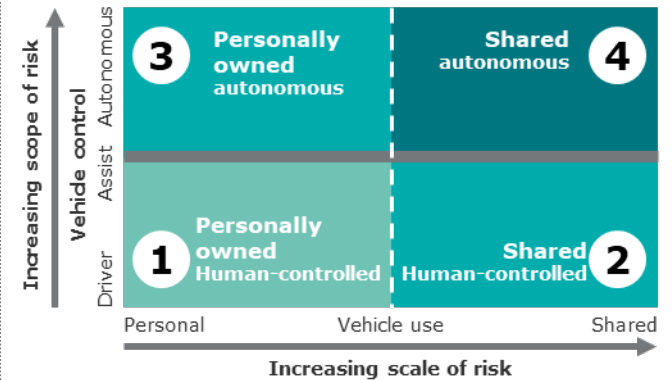
In each step towards a fully autonomous vehicle, different development and complexity stages of Advanced Driver Assistance Systems (ADAS) are used to set the technical foundation. Various sensors around the car detect obstacles, help keep the vehicle on track and warn the driver in case of danger. ADAS applications not only ensure a higher safety level for the driver by providing the vehicle with more information about its surroundings, but also promote comfort. The different stages of autonomous driving can be described in levels from 0 to 5, as defined by the Society of Automotive Engineers (SAE), adopted and further described by the National Highway Traffic Safety Association (NHTSA).⁵ The table below provides a summary of these levels, with example features from SAE.

	No Driving Automation	Driver Assistance	Partial Driving Automation	Conditional Driving Automation	High Driving Automation	Full Driving Automation
	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
	There is no automation at this level. All driving tasks are performed by the driver, even when enhanced by active safety solutions.	The vehicle is controlled by the driver, but the vehicle also has a few driving assist features that can provide, for example, steering OR braking/acceleration assistance.	The vehicle has combined automated features that can provide, for example, steering AND braking/acceleration assistance simultaneously, but the driver must remain engaged in the driving task and monitor the environment at all times.	The vehicle has an automated driving system capable of full control of the driving task; however, a driver is still a necessity. The driver must respond to requests to intervene and be ready to take control of the vehicle at all times.	The vehicle is designed to perform all driving functions under certain conditions. At this stage of automation, the driver may control the vehicle in limited conditions.	The vehicle is designed to perform all driving functions under all conditions. It may be optional for a driver to control the vehicle at this stage of automation.
Example features [SAE J3016]	<ul style="list-style-type: none"> Blind spot warning Lane departure warning 	<ul style="list-style-type: none"> Lane centering OR Adaptive cruise control (not simultaneously) 	<ul style="list-style-type: none"> Lane centering AND Adaptive cruise control (simultaneously) 	<ul style="list-style-type: none"> Traffic jam chauffeur 	<ul style="list-style-type: none"> Local driverless taxi Pedals/steering wheel may or may not be installed 	<ul style="list-style-type: none"> Same as level 4, but feature can drive everywhere in all conditions

In order to achieve higher levels of automations, OEMs, suppliers, software companies, regulators and other stakeholders have to solve a number of challenges, ranging from the development of reliable driving functionalities to settling remaining legal concerns while ensuring the safety, security and privacy of consumers.

The emergence of connected, electric, and autonomous vehicles and shifting attitudes around mobility are likely to profoundly change the way people and goods move about, and how they expect their data to be secured within this context. As these trends unfold, four concurrent “future states” could emerge within a new mobility ecosystem, emanating from the intersection of who owns the vehicle and who operates the vehicle.⁶ The future states present opportunities for safe and convenient mobility solutions, but also present unique data-related, cybersecurity challenges.

Future states of mobility and data-related risk



Although the use of shared vehicles is rapidly increasing along with higher levels of vehicle automation, personally-owned and human-controlled cars are still likely to exist concurrently with these future states – with both driver-controlled and autonomous vehicles sharing the road. Each future state presents new risks or increased potential impact.

Future State 1 | Personally-owned, human-controlled vehicles will continue to dominate the mobility system as owners will neither willingly part with their vehicles nor invest in new autonomous technologies with uncertain returns. As increased connectivity and new data-centric features are available to these vehicles, increased security capabilities will be required.







Future State 2 | Shared human-controlled vehicles experience continued growth as passengers value the convenience of point-to-point transportation and the demonstrated economic benefits of expansive car and ride-sharing. Use of mobile applications, connectivity to social media, and integration with payment systems increases the threats to these vehicles and their riders.

Future State 3 | Personally-owned autonomous vehicles will begin to prove safe, convenient, economical, and viable while consumers maintain a preference for private ownership. A new level of trust in communications is required not only within or directly around the vehicle, but with the surrounding infrastructure and the entire supply chain.

Future State 4 | Shared autonomous vehicles become a reality at the convergence of superior autonomous technology and the continued growth in shared mobility. The threats present at Future States 1-3 are increased by an order of magnitude due to the level of potential damage.

Global CAV testing and pilot legislation and standards

The progression of CAV testing legislation around the world is moving towards enhanced standards and more clear legislation. Similar to Ontario, there are other jurisdictions globally enacting or considering new CAV testing and innovation legislation:

 Germany	Autonomous Vehicle Bill was enacted in June 2017, modifying the existing Road Traffic Act defining the requirements for highly and fully automated vehicles, as well as addressing the rights of the driver. ⁷	 India	The laws (e.g., Indian Motor Vehicles Act, 1988) and rules regulating the operation of vehicles require a human driver to be in effective control of the vehicle at all times. The proposed Motor Vehicles (Amendment) Bill, 2017, has provisions to promote alternative technology and innovation while promoting safety on roads. ¹¹
 Australia	May 2017, Australian transport ministers agreed to the Guidelines for Trials of Automated Vehicles in Australia. The Guidelines provide a clear and nationally consistent approach with an aim to balance safety and innovation. ⁸	 China	January 2019, Over 101 license plates has been issued for Autonomous/self-driving cars. The Beijing government has issued license for testing autonomous cars on public roads, with a total of 123 kilometers for this test. Aside from Beijing, tests are performed in other cities around China including the provinces. Expectation is that 50% of vehicle sales in 2020 will come with autonomous functions. ¹²
 Netherlands	In November 2017, a draft bill was received by the house of representatives governing the experimental use of self-driving vehicles on public roads with remote drivers. The bill was eventually passed. ⁹ Companies that wish to test self-driving vehicles must first demonstrate that tests will be conducted in a safe manner through an admittance procedure run by the Dutch Vehicle Authority. The Dutch government recently announced a new driving license for self-driving cars with the aim of certifying new autonomous models and a framework for its legislation. ¹⁰	 Japan	The National Police Agency in December 2018 unveiled a draft bill that would allow vehicles with a high level of autonomous features to run on public roads. In May 2019, Japan released a bill allowing drivers to use their smartphones while their cars are traveling autonomously under certain circumstances and if they are able to shift to manual driving immediately during an emergency. ¹³

Ontario's Automated Vehicle Pilot Program

In 2016, Ontario launched a ten-year pilot program to allow the testing of automated vehicles on Ontario's roads.¹⁴ In response to advances in CAV technology, the program was updated on January 1, 2019 to allow for the testing and sale of more innovative technologies. These updates included:

- **Update to pilot restrictions:** AVs equipped with Society of Automotive Engineers (SAE) level 3 technology that are eligible and available for public purchase in Canada can now be driven on Ontario roads. These vehicles are no longer restricted to registered pilot participants. Vehicles with aftermarket SAE Level 3 technology (technology that has been added to a vehicle after sale, not by an OEM) remain restricted to the pilot program and are not permitted for public use. Anyone driving a vehicle with any level of automation continues to be required to be attentive at all times and obey all existing driving laws, including for distracted and impaired driving. Pilot participants can test driverless vehicles on Ontario's roads, under strict conditions that will ensure tests are conducted in safe and controlled environments.
- **Ontario's Cooperative Truck Platooning Pilot Program:** Ontario launched an eight-year pilot program to test connected "platooning" technology, in which large trucks are equipped with support systems and vehicle-to-vehicle communications that enable them to travel closely together as a group.¹⁵ To ensure safe testing, some of the requirements include having a strong carrier safety rating, having a trained and experienced driver in each vehicle, maintaining a safe gap between vehicles and following vehicle signage requirements.

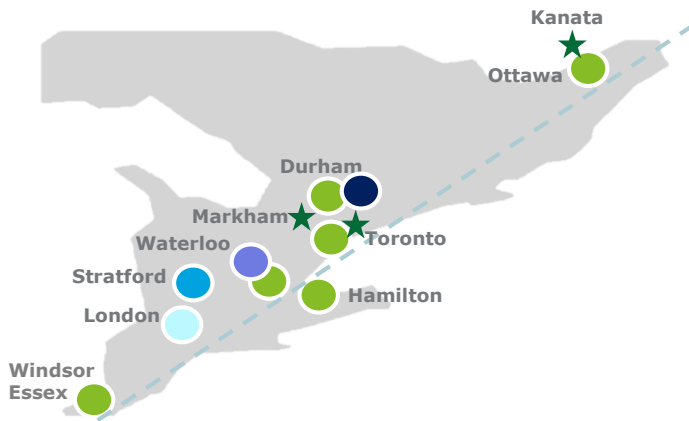
As part of the application processes for both pilot programs, applicants are required to declare the actions, design choices and measures they have taken to ensure the vehicles they plan to test have accounted for cybersecurity risks which can impact road safety.

Ontario's CAV innovation ecosystem

CAV testing and demonstration map

Ontario's CAV innovation is located along a similar corridor to Ontario's overall cybersecurity innovation, clustered close to academic centres, but with much more variation across Ontario and spilling into nearby jurisdictions.

Clusters of CAV testing and demonstration



Legend: Clusters of CAV testing and demonstration

- AVIN Regional Technology Development Sites (RTDSs)
- AVIN Demonstration Zone
- Automotive Centre of Excellence (ACE) at the Ontario Tech University
- National Research Council Canada space for manufacturing and automotive innovation
- Waterloo Centre for Automotive Research (WatCAR)
- ★ Industry Research and Initiatives/Pilots: GM (Markham), Ford (Kanata), Uber (Toronto), Kanata Autonomous Vehicle Cluster led by BlackBerry QNX (Kanata)



Deloitte's 2016 report on cybersecurity innovation "harnessing the cybersecurity opportunity for growth" found natural clusters of cybersecurity innovation in Ontario centred in the Greater Toronto Area, National Capital Region, and Kitchener-Waterloo.¹⁶

One of the key findings from the 2016 report on cybersecurity innovation was the geographic distribution of cyber SMEs that indicated natural clustering as a function of population, as well as:

- Confluence of academia and major industry within the GTA
- Significant military, security intelligence, and technology hubs in the NCR
- Technology-focused academic institutions (e.g., Institute for Quantum Computing) and anchor organizations (e.g., BlackBerry) in Kitchener-Waterloo

Clusters of cybersecurity innovation in Ontario



CAV cybersecurity innovation is occurring not only within academia and research settings, but within and in partnership with private sector organizations leading pilots and technology clusters in several innovation hubs and cities across Ontario.

CAV cybersecurity stakeholder landscape

The complex stakeholder ecosystem

The CAV ecosystem is made up of a variety of interconnected stakeholders, including automotive parts and software businesses, academic institutions, standards organizations, industry associations, and financial institutions.

The CAV cybersecurity stakeholders have unique interactions with regulators, policy makers, and economic development organizations across the CAV sector. The stakeholders included within this report span several sectors and sub-sectors, and many stakeholders have multiple roles.



In Ontario, while the largest number of CAV cybersecurity stakeholders are private sector organizations, many note the importance of partnerships with cities (e.g., City of Ottawa), the province (e.g., through AVIN), and the federal government through grants, technology clusters and corridors, and the development of standards and guidance.

Cross-provincial and cross-border partnerships have been also highlighted as important to the success of the CAV market, with an emphasis on the role the federal government should take in this industry.

The CAV cybersecurity ecosystem – Key examples across sector categories

Private Sector: Includes technology providers (such as infotainment, sensors, software development, and vehicle cybersecurity services), finance, insurance, automotive (including OEMs, Tier 1-3 suppliers, and fleet management).

Government: Includes government of all levels and regulatory bodies within Canada, including police and justice, ministries, public sector agencies, etc.

Academia: Includes post-secondary institutions (universities and colleges), research labs, and testing centres.

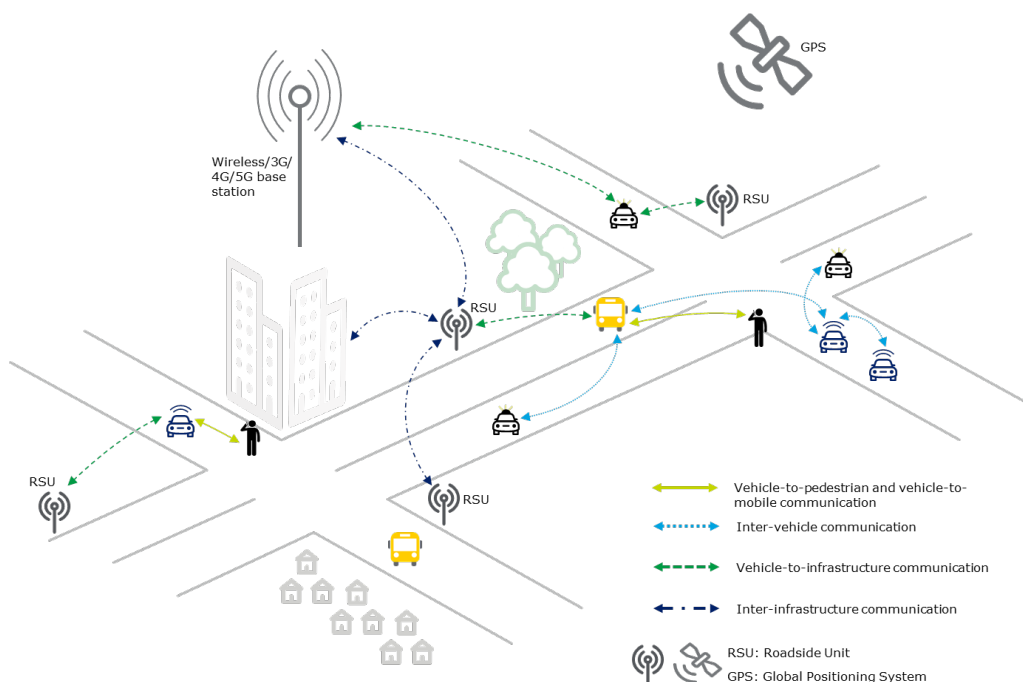
Associations & Standards Bodies Includes standards organizations and accreditation bodies such as National Institute of Standards and Technology (NIST), Society of Automotive Engineers (SAE), and International Organization for Standardization (ISO). Note that some standards bodies are part of, or funded by, public sector organizations, while others are industry-led and run.

CAV cybersecurity threat landscape: Attack vectors

Emerging attacks on CAVs – Increased remote attacks and communication channels

As the number and speed of communication channels with vehicles have increased, over the last few years there has been an increase in malicious attacks on vehicles. The number of cybercriminal attacks (“Black Hat”) has now surpassed the number of research-based attacks (“White Hat”) in this area, with the number of remote attacks surpassing physical attacks on vehicles – originating from increasingly long distances.¹⁷ This results in an increase in risks to the devices, the data being collected and shared by them, and the safety and privacy of the individuals whom the data is about.

CAV communication channels



CAVs face a combination of cybersecurity, physical safety and privacy challenges which consists of components unique to their ecosystem or larger in scale and impact – due to the number of communication channels and the volume and sensitivity of data transferred.

Key Attack Vectors¹⁷

- LIDAR and radar systems (e.g., spoofing or saturation attacks)
- Servers
- Keyless entry
- On-Board Diagnostics (OBD) port
- OBD dongle
- Mobile app
- Infotainment
- Broadband network (e.g., cellular)
- V2X communication
- Wi-Fi
- Sensors
- USB port
- Bluetooth
- Telematics Control Unit (TCU)

The top attack vectors as of 2018, according to an Upstream Security report,¹⁷ were remote server attacks (21%) and keyless entry attacks (19%), where an individual enters a car without using a key for either the door or the ignition. Another 10% of attacks were through the OBD port and 7% each were through mobile apps or infotainment systems.

Wi-Fi and cellular network attacks made up just above 4% each, but could grow in the context of increased connectivity and 5G coverage. With 41% of Black Hat incidents involving back end servers in 2019, including breached OEM web servers, there is a need not only for device security and safety, but also for a full ecosystem, strategic approach to threats.

CAV cybersecurity threat landscape: Risk vectors



Organizational risks to the CAV ecosystem

A CAV is a combination of connected devices in a single moving device – with a large threat landscape. The complex CAV ecosystem contains some emerging challenges that are impacting the organizations operating in this sector.

Blending Realms of Physical and Cybersecurity

In a dynamic and connected IoT environment, new and existing technology platforms can expose an organization to security risks of a converged nature.

Data Security and Privacy

Protecting customer, employee, and organizational data requires advanced security controls while ensuring data integrity and privacy requirements are considered and designed at the outset.

Attacker Sophistication

While the rapid growth in Artificial Intelligence (AI) has helped organizations, it has increased the capacity of threat actors, enabling higher effectiveness of attacks.

Collaboration

With physical security becoming increasingly technology enabled, breaking silos and collaboration amongst the security teams can optimize threat management.

Risk Culture

Having the right risk culture is one of the key success factors in preparing for and tackling new risks.

Talent

Recruiting, training and retaining top cybersecurity talent.

Enterprise View

Addressing risks using an enterprise lens provides a holistic view of risk which is needed to tackle today's emerging threats.

Regulation and Justice

Understanding and updating the regulatory and justice framework is needed to ensure a safe and secure CAV ecosystem.

Key threats impacting the CAV ecosystem



Insider Threats: Insiders are trusted, have knowledge and access to the organization's crown jewels. Insider's motivations may vary – they may steal data, commit fraud or cause physical harm or sabotage. Detecting insiders behaving normally, but with ulterior motives, can be challenging – highlighted by cases like the Levandowski trade secret trial between Waymo and Uber.¹⁸



Cyberattacks into V2X Communications: With far more on-board software needing regular security and navigational updates, autonomous vehicles in the new mobility ecosystem will likely have communication lines back to the manufacturer for instant transmission of software-related patches. Vulnerabilities in the communication channels could result in a threat actor compromising the safety and security of the vehicles.



Hijacking Vehicle Sensors and Taking Over Physical Controls: The intersection of critical and noncritical vehicle sensors and the underlying busses can allow a message injector to pass unwanted data to devices in the vehicle by exploiting the weakest link. Advances in cognitive computing are creating new avenues to exploit the sensors and IoT devices used by CAVs as demonstrated by researchers in tricking the vehicle LIDARs to make inaccurate judgements, by using spoofing and saturation attacks. This can lead to physical CAV crashes or CAV thefts.



Dumpster Diving for Data: Just as flight data recorders collect information about what happens in a cockpit, connected vehicles absorb details about what their owners and passengers do, which can act as a honeypot for malicious actors. Furthermore, there have been reported cases where drivers of ride sharing apps have secretly recorded their passenger conversations, with privacy ramifications.



Supply Chain and 3rd Party Risks: The CAV ecosystem consists of a large variety of service and solution providers. Managing 3rd party risks across the value chain has been challenging for organizations due to the different maturity levels of the service providers, lack of visibility and control of data, and difficulties enforcing a common standard of security control requirements.

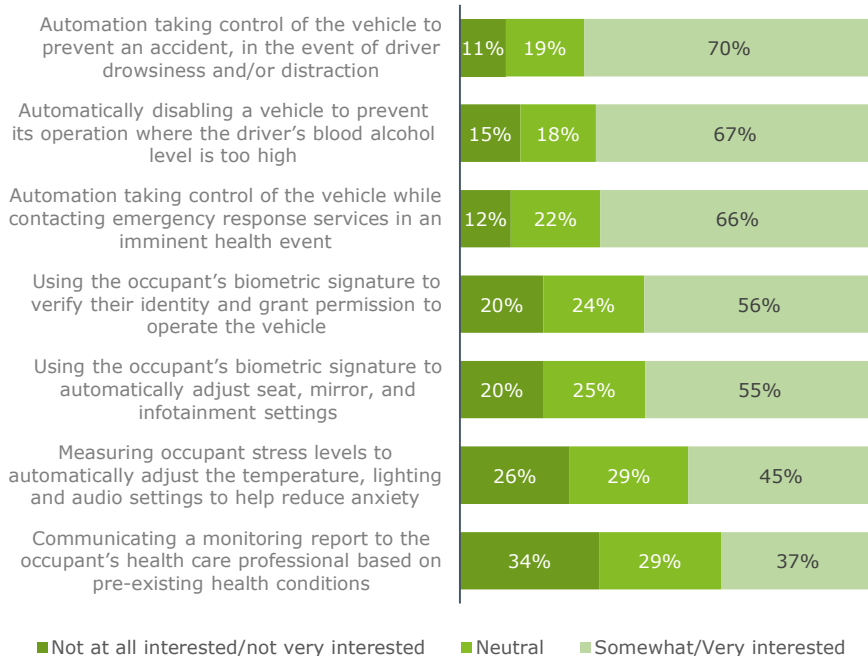
CAV cybersecurity threat landscape: CAV data collection

Consumer trust and vehicle data collection

Growing consumer expectations for connected and available services, such as smart safety features and location services, has come along side a consistent lack of consumer trust in how their data is handled once collected through vehicles.

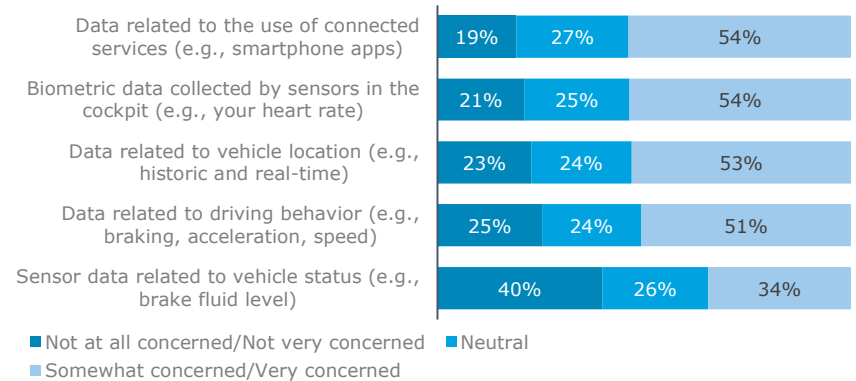
Deloitte's 2019 Global Automotive Consumer Survey – which surveys 25,000 consumers across 20 different countries annually to identify trends in the automotive industry across countries and generations – reports that **only 27% of Canadian consumers trust OEMs in managing the data that is generated in a connected vehicle**, but more than two-thirds of Canadian consumers are interested in benefits of connected vehicles.¹⁹ To provide these benefits, CAV service providers need to exchange a large volume of data – potentially sensitive data – with the vehicle over time and across geographies.

As vehicle interiors are equipped with more connected sensors and/or autonomous driving technology, how interested are you in each of the following?

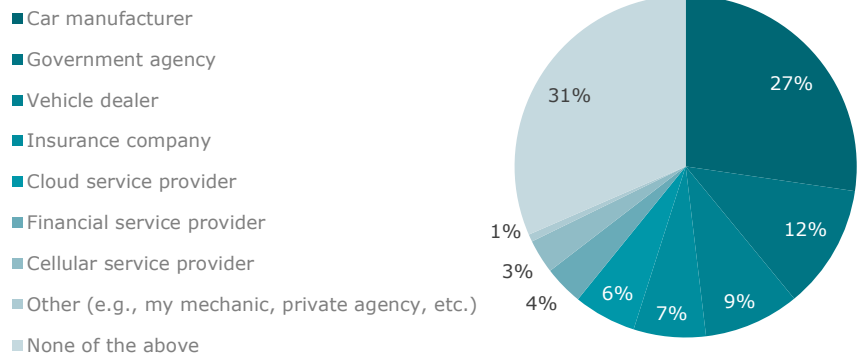


In the context of users finding more benefit to connected vehicles year-over-year, 45% of these consumers think it is at least somewhat important to have the same technology interface across multiple vehicles – **more than half of consumers reported concerns where data related to apps, biometrics, and the vehicle's location is collected and shared.** There are **real concerns about vehicle attacks when connected via wireless Internet** – remaining consistent over the past two years, despite the growing perceived value of connected vehicles. Consumers' level of trust varies by the type of organization handling their information.

How concerned would you be if the following types of data were shared with your vehicle manufacturer, dealer, insurance company and/or other third parties?



Which of the following entities would you trust the most to manage the data being generated and shared?



CAV cybersecurity threat landscape: Trends and impacts

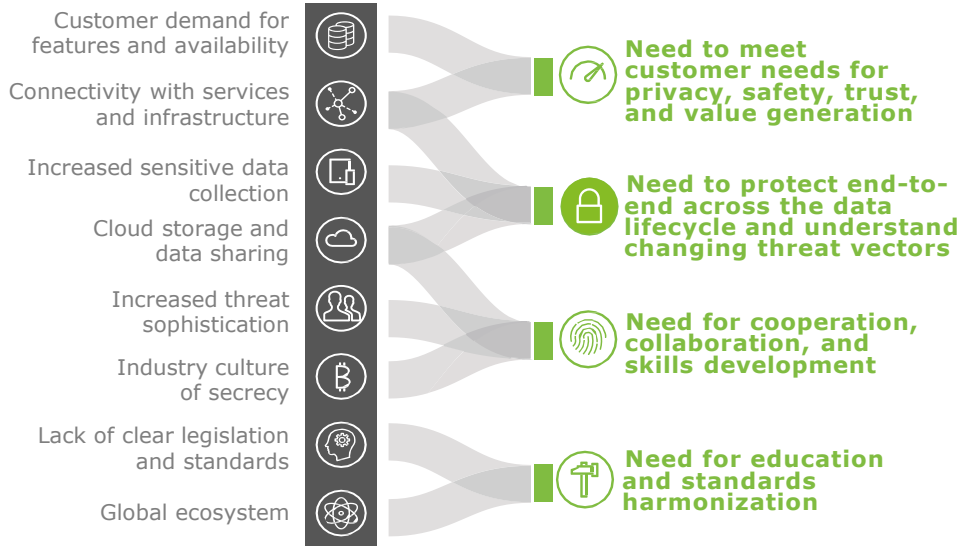
CAV cybersecurity trends and impacts on consumers and industry

As the number and sophistication of cybersecurity threats increase globally, this has immediate impacts on the growing CAV industry. Consumers are driving the demand for better connected, integrated vehicle services, but as more sensitive information about vehicles and their occupants is being collected and shared in an interconnected ecosystem of manufacturing and service providers, vehicles are increasingly a valuable target for threat actors. The industry landscape is changing in response to consumer and cyber demands, but stakeholders are still hesitant to cooperate in a competitive market that relies heavily on trade secrecy.



It is in this context that the cyber threat landscape continues to evolve and take advantage of CAV vulnerabilities, including a lack of standardization across global regulations.

CAV cyber trends impacting existing risks and creating ecosystem needs



Threat influences and impacts to CAVs in Ontario

Key factors influencing cybersecurity risk in smart cities (from Deloitte's report *Making Smart Cities Cybersecure*²⁰):

- **Convergence:** Convergence of information technology (IT) and Operational Technology (OT) infrastructures, blurring the divide between the physical and cyber worlds
- **Interoperability:** Coexistence and frequent interactions between old and new systems and platforms
- **Integration:** Integration and comingling of services across domains through IoT and digital technologies

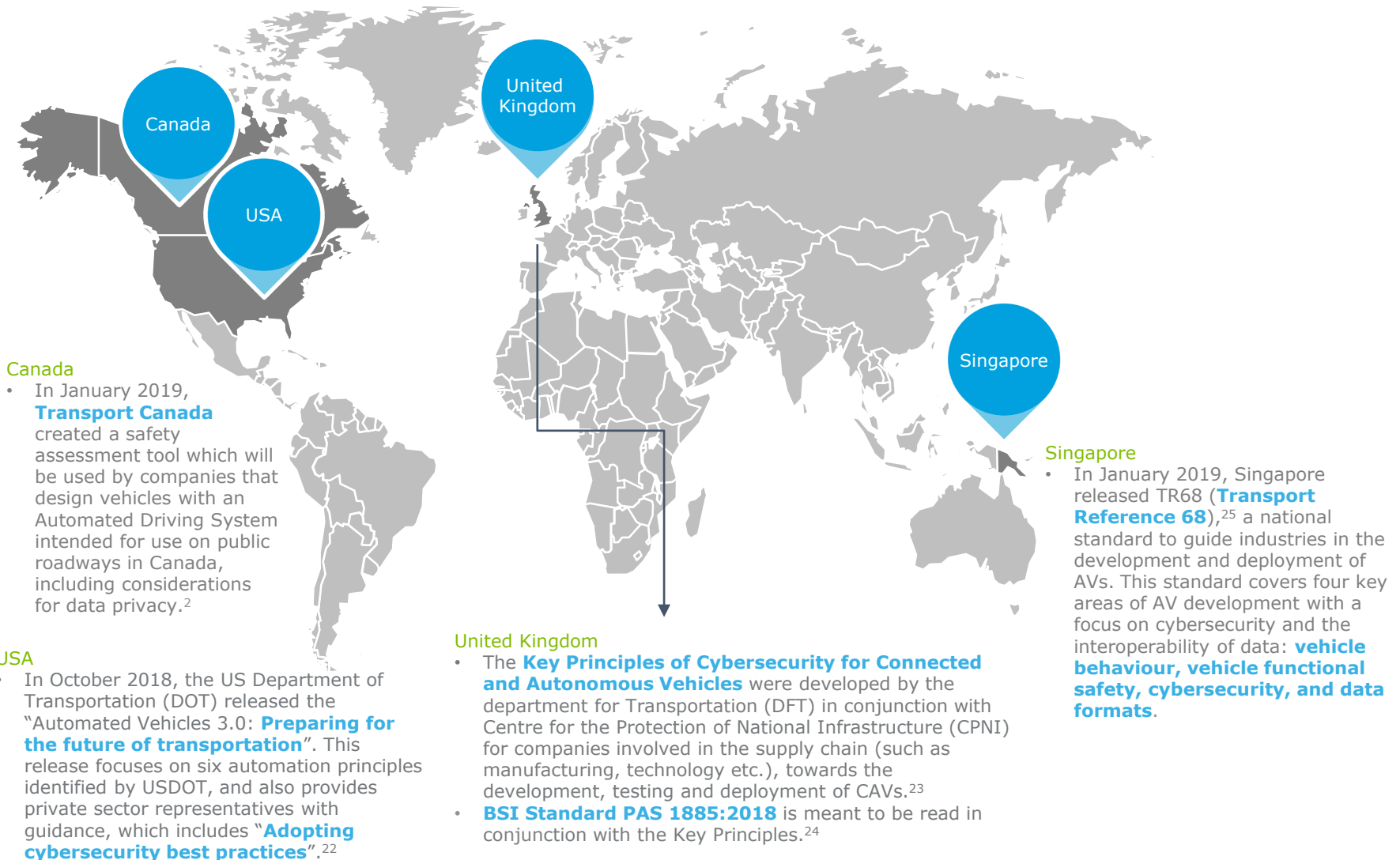
Key impacts of threats to consumers using networked vehicles (from Deloitte's report *Securing the Networked Vehicle*²¹):

- **Theft of property:** Malicious actors might steal vehicles for personal or financial gain. Cargo theft in Canada amounts to \$5 billion CAD in economic losses per year and is further facilitated if attackers can access a vehicle's location, route, or password
- **Theft of data:** Connected vehicles may capture and store a range of personal information, including transaction and payment information, user credentials, and communications
- **Physical destruction and sabotage:** If remote control of a vehicle or access to its location and route is possible, a malicious actor can seriously damage the vehicle, its passengers, or surrounding property
- **Invasion of privacy:** Personal information, metadata, home and work address, and communications via mobile phone could be captured through CAVs and accessed without permission
- **Fraud:** Vehicle insurance fraud could be a significant issue as insurance estimates increasingly rely on vehicle data and as vehicle sharing increases in prevalence

The top impacts in 2019 of cyberattacks on vehicles were **unauthorized control over car systems, car theft, and data breaches**.¹⁷ This demonstrates that cyberattacks have impacts beyond traditional network security attacks and extend to real impacts on human lives.

Global cybersecurity developments in the CAV landscape

We identified cybersecurity legislation and requirements development around the world relevant to the CAV ecosystem.



Cybersecurity embedded in CAV strategies and legislation

In Canada and globally, governments are increasingly considering and embedding cybersecurity into their CAV strategies, assessment tools, and laws.

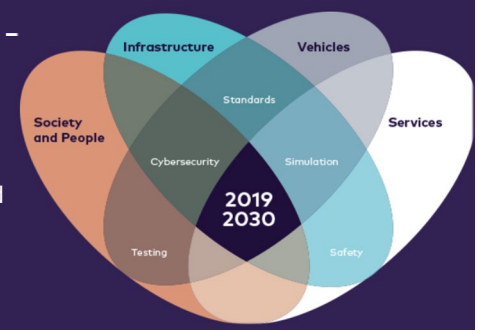


Trend: Formalizing best practices

A number of countries are drafting legislation and releasing guidance and frameworks meant to improve the research, development and testing of CAVs, with more countries beginning to consider cybersecurity as a key component to these laws, strategies, and guidance – including Canada, USA, and the UK.

Cybersecurity as a core component for a CAV roadmap – A spotlight on the UK

Zencar (formerly Meridian Mobility, developed by the UK government) will focus on key areas of UK capabilities in the global CAV sector, including advanced development and validation, connected environments, data, cybersecurity, and new service development. In September of 2019, they will launch their 2019-2030 roadmap: **The UK Connected and Automated Mobility Roadmap to 2030**, which includes cybersecurity as a key component.



Canada

Ontario co-chaired the development of a Canadian policy framework for CAVs, released in January 2019,² which defines a set of policy principles that Canadian government bodies at all levels may use as a guide to promote the testing and deployment of CAVs across Canada. This framework highlighted both cybersecurity and privacy as important vulnerabilities, and recommended increased public awareness of these considerations.

Transport Canada created a safety assessment tool which will be used by companies that design vehicles with an Automated Driving System intended for use on public roadways in Canada.² This assessment tool's outcome is grouped into three sections which include cybersecurity and data management, including considerations for data privacy.



Singapore

The Singapore government made an amendment to its *Road Traffic Act* which allows self-driving cars to be tested on public roads in 2017.²⁶ The Ministry of Transportation released a series of Autonomous Vehicles (AV) Rules in February 2017 to allow for self driving cars²⁷. In addition, the Singapore's national standards for AVs, TR68, was created to promote safety in the development and deployment of AVs in Singapore.²⁸



United Kingdom

The UK has set up a government department, the Centre for Connected and Autonomous Vehicles, that is working on legislation to allow testing on motorways in the country. There are also testing schemes in cities, including London and Coventry, with research organizations established to develop the technology and systems. **The UK Connected and Automated Mobility Roadmap to 2030** includes cybersecurity as a key pillar (see spotlight above).²⁹



United States of America

Since 2014, United States has shown a great increase in legislation across its states with regards to autonomous or highly autonomous vehicles. There are cities where autonomous vehicles have already been deployed and are presently running (e.g., Ann Arbor). Federal rules development is beginning to include privacy and cybersecurity plan requirements (e.g., SELF DRIVE Act, not yet passed by the Senate),³⁰ and records show that as of 2018, 15 states have enacted 18 CAV related bills.³¹

Industry-driven cybersecurity standards and regulations



Industry-driven Standards Formalization

Industry associations and standards associations around the world are developing important cybersecurity guidance with direct applicability to CAVs:

- **ISO and SAE** are developing a new joint standard "ISO/SAE 21434 Road Vehicles – Cyber Security Engineering". This standard is currently in progress.
- **Singapore Standards Council's (SSC's)** Manufacturing Standards Committee, Land Transport Authority, and Singapore Manufacturing Federation-Standards Development Organisation (SMF-SDO) supported the development of Technical Reference 68 (TR68) standards for autonomous vehicles.
- **The British Standards Institution PAS 1885:2018** is meant to be read in conjunction with the UK's Key Principles of cybersecurity for Connected and Autonomous Vehicles.²³
- **NIST's cybersecurity for the Internet of Things (IoT) Program:** "Considerations for a Core IoT Cybersecurity Capabilities Baseline" was released in February 2019. As a follow up to NIST IR 8228, this initiative will involve a collaboration between NIST and stakeholders to develop a cybersecurity baseline – a set of core capabilities that can be broadly applicable to many or all pre-market IoT devices.⁴



Spotlight on proposed UN Regulation on CAV Cybersecurity

In support of the United Nations Economic Commission for Europe (UNECE) World Forum for Harmonization of Vehicle Regulations (WP29) Working Party on Automated/Autonomous and Connected Vehicles mandate, experts of the Task Force on Cyber Security and Over-the-air issues submitted a new draft Regulation on CAV Cyber Security in November of 2018.³²

Organizational security and **governance** at the highest level

Secure **storage** and **transmission** of data

Security **risk assessment** and management, including across the supply chain

Vehicle manufacturer **testing** procedures on security functions

Cybersecurity **monitoring** and incident response

Security of software managed throughout its **lifetime**

Third party risk management and cooperation on security

Vehicles should be designed with the capability to **detect** cyberattacks and respond appropriately

Vehicles should be designed using a **defence-in-depth** approach

The vehicle should be designed to be **resilient** to cyberattacks

Key cybersecurity principles

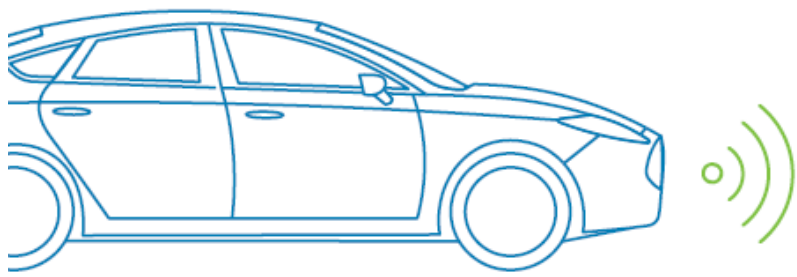
The proposed UN Regulation develops uniform provisions concerning the approval of cybersecurity, and includes requiring those Contracting Parties to have an Approval Authority or Technical Service assess and issue "Cyber Security Management System Certificates of Compliance".

Solution developments in the CAV landscape ○

Partnerships and collaboration between CAV stakeholders are moving CAV innovation forward, in the face of emerging risks.

CAV innovation and the mantra of cooperation

Research on the intelligence and logic for CAVs began as early as the 1970s. The foundations of the networked mobility era was laid by the PROMETHEUS project launched in 1986 by Mercedes-Benz and EUREKA (a pan European intergovernmental organization for international cooperation in innovation) and paved way for technologies such as cruise control and V2X communications.³³



Over the last few years, there have been increasing partnerships between global organizations as companies race to the finish line to launch vehicles with increasing autonomous capabilities and share the development costs. Below is an illustrative list of some of the recent, major partnerships in the CAV space:

- Honda in Oct 2018 has committed to invest \$2.75B in GM's Cruise autonomous unit to jointly develop self-driving fleet.³⁴
- Waymo (formerly Google self-driving car project) has partnered with Fiat Chrysler in early 2018 to add up to 62,000 Chrysler minivans to Waymo's fleet as well as 20,000 cars from Jaguar Land Rover.³⁵
- Building on previous investments, Toyota led a \$1B funding in Apr 2019 into Uber's Advanced Technology Group to accelerate commercialization of automated ridesharing services.³⁶
- In Feb 2019, BMW and Daimler announced cooperation on driverless technology complemented by investing \$1B into a joint venture to develop mobility services.³⁷

Emerging technology risks and solutions for CAVs

The use of emerging technologies such as blockchain, 5G and 3-D printing brings with them both challenges and opportunities to the cybersecurity of CAVs.

For example, blockchain solutions can be used to share data between CAVs, OEMs and service providers enabling decentralized information management and deriving valuable insights using AI and Machine Learning (ML). At the same time, blockchain introduces traditional cybersecurity challenges such as implementation of effective key management practices, as well as technology-specific challenges such as the risk of collusion, which needs to be monitored and prevented.

5G networks, with their ultra-low latency and increased speeds, are poised to act as an enabler for hyper connected CAVs and V2X communications. As the volume of data collected and processed grows, the challenges it poses to user privacy should be carefully addressed, and due diligence should be performed to ensure the security of 5G infrastructure and architecture.

Additive manufacturing, also known as 3-D printing, provides more process and energy efficient means to creating automotive components. Researchers have demonstrated that by maliciously manipulating the 3-D blueprint software code, it is possible to induce mechanical failures in 3-D printed objects.³⁸ As the mainstream adoption of such technologies increases, suppliers should ensure security by design principles are embedded in all the manufacturing stages.

Implications to cybersecurity of CAVs

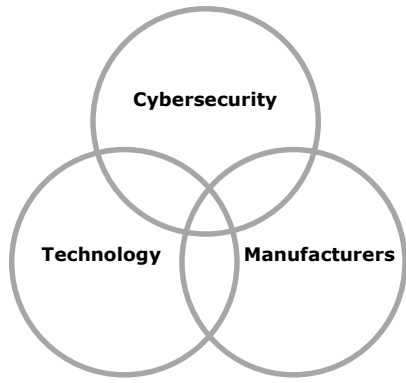
Increased collaboration and adoption of security and privacy by design principles amongst the players will enable knowledge transfer, acceleration of technology development, and help the cause of enhancing CAV cybersecurity posture.

Cybersecurity innovation models in the CAV ecosystem

Key trends from CAV innovators – areas of focus and emerging synergies between previously siloed industries.

A collaborative approach to CAV cybersecurity innovation

Across the start-up and development community, innovation across cybersecurity, technology, and manufacturing experts that had traditionally occurred in siloes is converging.



Collaborative approach

Cyber start-ups offer expertise to manufacturers and work with technology start-ups to build technologies that efficiently address cyber threats (e.g., integration of AI technologies).

Trends in CAV cybersecurity and privacy innovation

In order to develop cybersecurity solutions tailored to the CAV ecosystem, technology and cybersecurity companies are developing innovative partnerships with manufacturers across the supply chain. In some instances, these cyber solutions do not require internet connections, reduce possible threat vectors, and use AI and Blockchain technologies to provide more efficient cybersecurity solutions.

Trends in the CAV cybersecurity innovation ecosystem include:

Partnerships and Proof of Concepts (POCs) with manufacturers



In specific instances, no internet connection required to provide cyber protection



Innovation in cybersecurity using AI and blockchain



Moving from ideas, to development, to market

New solutions in the CAV ecosystem are moving from ideas, to product and service development, and finally to market – iterating on key scale and implementation challenges.



Ideas innovation

Understanding needs and getting the right focus

Research and ecosystem analysis to identify key cybersecurity risks and challenges, and what is needed to successfully mitigate them.



Solution development

Getting the concept right

Turning innovation into reality through research, testing, and development; looking to launch in the market.



Market innovation

Scaling the solution

Once the solution is refined and ready for market, innovating to meet interoperability, scale and other implementation challenges.

See the Appendix for a list of global solution developments in CAV cybersecurity.

CAV cybersecurity considerations: Top stakeholder themes

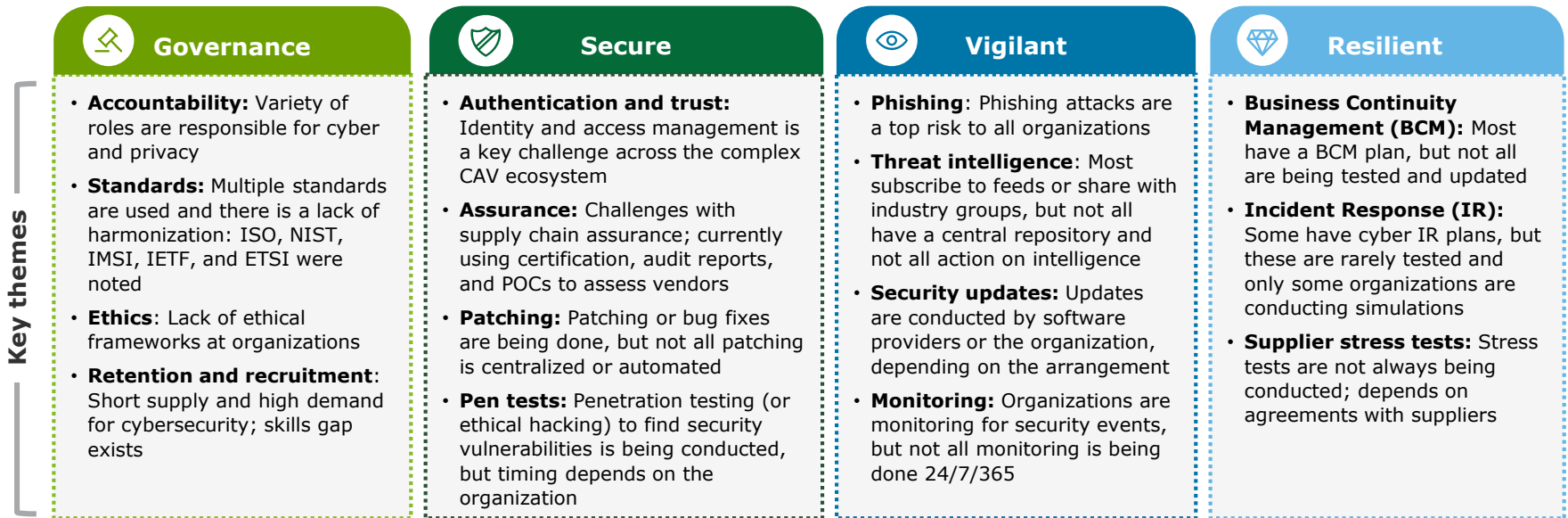
Key themes from stakeholders across the extended ecosystem

When asked about cybersecurity CAV risks, through interviews and surveys, private sector organizations highlight key risks across the extended security perimeter – with a focus on cloud connectivity, peer-to-peer communication, infotainment systems, safety systems and data stored in vehicles. The main lesson learned from CAV stakeholders and global research is that the entire extended security perimeter must be considered, with a focus on cloud, in-vehicle, and network security.

Authentication and trust are some of the key considerations

While the defence-in-depth approach is good in principle, several CAV sector stakeholders across the extended ecosystem describe the challenges around layering patchwork security safeguards onto legacy systems and devices. This is particularly an issue in the context of a complex supply chain, where there is difficulty ensuring that products and services across the lifecycle are secure, that they are what they say they are, and that communications between devices are authentic.

Key themes stakeholders identified in interviews and survey responses are categorized below under the Deloitte CSF pillars:



"Lack of certification, lack of coordination with other jurisdictions. There are many guidelines and standards, but nothing to certify to, so everything is subjective."
[stakeholder]

Stakeholders report the following CAV components are most at risk along the extended security perimeter:

- Infotainment systems
- Connectivity to cloud services
- Peer-to-peer communication (V2V)
- Safety and control systems
- Vehicle-stored information

"Protection of the end-to-end traffic flow and resilience from multiple attack vectors" is one of the biggest CAV cybersecurity challenges
[stakeholder]

Key global considerations for CAV cybersecurity

One of the key considerations for CAV cybersecurity globally is the standardization and coordination with other jurisdictions on requirements – stakeholders want to have a clear and objective standard to certify to. Stakeholders across sectors and jurisdictions identified opportunities to collaborate across government and industry to create harmonized standards, and to team up with a certification authority to develop security standards and issue certifications – similar to what is currently done for functional automotive safety requirements.

Stakeholders across the CAV landscape are identifying cybersecurity as a critical component to ensuring the safety and security of the future of mobility. The Canadian Government authorities have signaled that they may need to play a larger role in enforcement or auditing against privacy and security requirements in the context of emerging technologies like CAVs,² and have invited stakeholders to work together on developing future policy frameworks and guidance.

"Now more than ever before, cybersecurity is top of mind for automakers as their cars become more connected to the outside world. Today's vehicles are computers on wheels—with over 100 million lines of software per car. The technology in them protects us, entertains us, and in many ways is beginning to drive us – think ADAS features like collision avoidance, blind spot monitoring and lane departure warning systems that are fast becoming de rigueur among automakers with one eye on the future.

However in the race for self-driving cars, building consumer trust when it comes to safety is just as important as building the technology. For the general public to accept and ultimately adopt autonomous vehicles en masse, there needs to be trust in the technologies, trust in their advantages and of course, trust that the companies building them (and profiting off of them) will act responsibly.

It is a moral imperative for those of us within the industry that are advancing this fast approaching future to make sure it is both safe and secure."

– BlackBerry

Biggest opportunities for CAV cybersecurity



Standardization, certification and legislation

Creating a clearer picture of which standards and guidelines to follow, and the development of a certification process and/or new legislation to audit and/or enforce key standards. In Canada, significant work is underway through Transport Canada to develop and adopt standards for many aspects of CAVs as well as discuss the development of a certification process for CAV operations. Working together with ISED, Transport Canada launched a Vehicle Cyber Security Working Group to discuss such considerations and possible solutions with CAV experts.



Skilled talent growth and retention

With leading universities and academic test centres, there is an opportunity to better retain cyber talent in the automotive industry – such as through meaningful partnerships between academia and industry.



Collaboration and partnerships across industries

Collaboration of multiple players from different industries to innovate in the CAV space – from cybersecurity companies, to OEMs, to telecom and payment innovators.



Bringing OEM and technology innovation to market

The existing presence and innovation across OEMs and technology companies active globally is seen as a significant advantage – and should be fostered for growth in this space. Moving CAV cybersecurity research and development sustainably into the market should be a focus.



Trust and authentication innovation

Developing trust and authentication processes and tools for CAVs, leveraging architectures that are secure by design (e.g., with pre-existing security capabilities to enforce authentication and integrity).



Convergence security testing

Converting and expanding existing and new testing sites into convergence security testing facilities to ensure that the range of cybersecurity threats – within and near the vehicle, and interactions with surrounding infrastructure – are considered before a CAV is available on the market.



Privacy and security by design; ethical frameworks

Ensuring privacy and security features are designed into new solutions, to help manage emerging privacy and security risks for increasingly connected and autonomous vehicles. Develop and incorporate ethical frameworks into the solution development lifecycle at organizations. For example, the Office of the Privacy Commissioner of Canada (OPC) is developing privacy guidance for consumers of connected vehicles and planning to develop guidance for the broader CAV ecosystem over the next few years.

Key opportunities for CAV cybersecurity in Ontario ○

Ontario's key CAV cybersecurity considerations

The connected vehicles space is growing and further highlighting the importance of cybersecurity to CAV innovation and market growth. In the context of emerging threats, there are some key considerations that add complexity to being able to respond to and manage CAV cybersecurity risks. These include the lack of clarity around standards, difficulty training and retaining skilled resources in this industry in Ontario, collaboration across a highly competitive industry, and gaining and maintaining trust – not only with customers, but in the products themselves and their continuous communications with individuals and objects in the surrounding ecosystem.

Ecosystem Themes	Key Considerations
Standardization & Enforceability	<p>Absence of unified requirements:</p> <ul style="list-style-type: none"> • Many different international and local standards • No certification required presently in Canada • Lack of clear regulatory requirements and enforcement • Expansive supply chain and ecosystem of different suppliers and service providers (e.g., telecomm, payments) with different requirements
Training & Development	<p>Difficulty attracting and retaining cyber talent:</p> <ul style="list-style-type: none"> • High demand and low supply for cybersecurity talent • Difficulty retaining talent in this industry • Lack of clear translation between academic work and sustainable industry positions
Transparency & Collaboration	<p>Lack of transparency and cooperation on cybersecurity challenges within the automotive industry:</p> <ul style="list-style-type: none"> • Gap between research/academia and industry • Lack of sharing between different OEMs and service providers due to competition • Lack of transparency on key cybersecurity challenges due to risk of vulnerabilities being exposed to competition or malicious actors
Trust	<p>Difficulty ensuring assurance of products and services across the supply chain and trust of providers and communications, due to the complexity of the environment and required communications (e.g., V2I, V2V) to allow a CAV to navigate and receive updates.</p>

Key opportunities to move CAV cybersecurity forward in Ontario

Organizational privacy and security awareness and increased maturity



Helping Ontario organizations better understand cybersecurity risks and gaps, their responsibilities, and how to design privacy and security into their products or services and organization, through training and awareness. For example, Ontario co-chaired the PPSC CAV policy framework development², highlighting the need for awareness.

Cross-border partnerships for CAV cybersecurity



Promoting strategic investments and operational partnerships with different governments, academic centres, cybersecurity hubs, and industry across borders.

CAV cybersecurity internships and job placements



Supporting lasting industry partnerships for training and retaining top cyber talent in the automotive industry. In Ontario, the government funds various programs, such as the AVIN Talent Development program, and has further signaled its commitment to harnessing and developing talent in the automotive industry through its automotive sector plan, *Driving Prosperity*.³⁹

Standardization and a certification process for CAV cybersecurity



Working across all levels of government to participate in the development of new, harmonized laws and guidance to provide clarity on national standards and responsibilities, and to reduce barriers to innovation while promoting secure product and service development. For example, Ontario CAV stakeholders and policy leaders continue to participate in cybersecurity working groups to provide their perspective on how best to develop and establish important frameworks for CAVs.

Research, testing and development of CAV cybersecurity



Expanding existing labs and vehicle testing centres to accommodate cybersecurity testing will accelerate progress in this field and attract talent and industry leaders. For example, through Ontario's AVIN R&D partnership fund program, CAV stakeholders have the opportunity to partner and collaborate to develop, test and commercialize new technologies in the CAV space. The Automotive Centre of Excellence (ACE) at Ontario Tech University is bringing cybersecurity research into practice by beginning to incorporate cybersecurity testing into their facility. *For more information on convergence opportunities at testing centres, see the Appendix.*

Conclusion



CAV cybersecurity requires collaboration across the entire CAV ecosystem

Conclusion

Connected and autonomous vehicle technology has the ability to enhance the safety and effectiveness of mobility. Yet, the growing CAV industry is faced with a number of emerging cybersecurity threats – across the full supply chain – compounded by the increase in both physical and digital touchpoints.

Together with complex technical, regulatory, and organizational considerations, CAV ecosystem stakeholders will need to work together to manage and get ahead of cybersecurity threats. To do so, cybersecurity in the CAV ecosystem needs to be a collaborative effort, rather than growing and developing in silos.

Collaboration includes partnerships across various industries and specializations, collaboration with and across governments by developing approaches to standardization and enforcement in CAV industries, and collaboration with academia, to create and enhance test centres, research, and talent development to better understand physical and cyber threats to CAV technology.

Next steps for Ontario

Ontario CAV cybersecurity stakeholders are telling us there is still a way to go in terms of clarity on requirements, partnerships, and support for CAV cybersecurity – but there are a lot of opportunities to continue to establish Ontario as the go-to market for this core component to the success and adoption of CAVs around the world.

For example, through AVIN, the Government of Ontario has been taking key steps towards developing these opportunities and facilitating growth in Ontario. As CAV cybersecurity continues to grow in importance and gain traction across governments, industry and academic leaders, and the public, AVIN is looking forward to continuing to engage with the entire CAV ecosystem to enable the future of CAV cybersecurity in Ontario.



Endnotes

1. *Automated and Connected Vehicle 101. Transport Canada 2019.* Available at: <https://www.tc.gc.ca/en/services/road/innovative-technologies/automated-connected-vehicles/av-cv-101.html>
2. *There have been a number of recent federal Canadian developments, including:*
 - *Driving Change: Technology and the Future of the Automated Vehicle. Senate of Canada 2018. Report of the Standing Senate Committee on Transport and Communications.* Report available at: <https://sencanada.ca/en/info-page/parl-42-1/trcm-driving-change/>
 - *Safety assessment for Automated Driving System in Canada. Transport Canada 2019.* Available at: https://www.tc.gc.ca/en/services/road/documents/tc_safety_assessment_for_ads-s.pdf
 - *Automated and connected vehicles policy framework for Canada. PPSC Working Group on Automated and Connected Vehicles 2019.* Available at: http://publications.gc.ca/collections/collection_2019/tc/T42-13-2019-eng.pdf
 - *Statement by Minister Bains and Minister Gould on the Privacy Commissioner findings on Facebook privacy practices. ISED Canada 2019.* Available at: <https://www.canada.ca/en/innovation-science-economic-development/news/2019/04/statement-by-minister-bains-and-minister-gould-on-the-privacy-commissioner-findings-on-facebook-privacy-practices.html>,
 - *Canada's Digital Charter in Action. Government of Canada 2019.* Available at: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html
3. *World Economic Forum Global Risks Report 2019. WEF 2019.* Available at: <https://www.weforum.org/reports/the-global-risks-report-2019>
4. *Consideration for managing IoT Cybersecurity and Privacy Risks. NIST 2018.* Available at: <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8228-draft.pdf>. Further information available at: <https://www.nist.gov/blogs/i-think-therefore-iam/dont-leave-us-our-own-devices-seeking-feedback-draft-nistir-iot>, and <https://www.nist.gov/blogs/i-think-therefore-iam/lets-talk-about-iot-device-security>
5. *SAE International Releases Updated Visual Chart for Its "Levels of Driving Automation" Standard for Self-Driving Vehicles. The Society of Automotive Engineers (SAE) 2018.* Available at: [https://www.sae.org/news/press-room/2018/12/sae-international-releases-updated-visual-chart-for-its-\"levels-of-driving-automation\"-standard-for-self-driving-vehicles](https://www.sae.org/news/press-room/2018/12/sae-international-releases-updated-visual-chart-for-its-\). For the detailed taxonomy, also see: *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_201806.* Available at: https://www.sae.org/standards/content/j3016_201806/. For a summary of the SAE levels of driving automation, also see: *Automated Vehicles for Safety – The Road to Full Automation. National Highway Traffic Safety Administration (NHTSA) 2019.* Available at: <https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety>
6. *Securing the future of mobility. Deloitte 2017.* Available at: <https://www2.deloitte.com/insights/us/en/focus/future-of-mobility/cybersecurity-challenges-connected-car-security.html>
7. *The state of autonomous legislation in Europe. Auto Vista Group 2019.* Available at: <https://autovistagroup.com/news-and-insights/state-autonomous-legislation-Europe>
8. *Australian trials and policy development. Australian Government 2017.* Available at: <https://www.austrade.gov.au/future-transport/connected-automated-vehicles/>
9. *New legislation allows for testing of cars with remote drivers. Government of the Netherlands 2017.* Available at: <https://www.government.nl/latest/news/2017/11/22/new-legislation-allows-for-the-testing-of-cars-with-remote-drivers>
10. *Bikes but spanner in works of Dutch driverless car schemes. The Guardian 2019.* <https://www.theguardian.com/world/2019/feb/13/bikes-put-spanner-in-works-of-dutch-driverless-car-schemes>
11. *Centre to reintroduce motor vehicle bill in-house. Hindustan Times 2019.* Available at <https://www.hindustantimes.com/india-news/centre-to-reintroduce-motor-vehicle-bill-in-house/story-Jn6p2G7BGflapEglgSuiL.html>
12. *Autonomous vehicles gaining more ground. China Daily 2019.* Available at: <http://www.chinadaily.com.cn/a/201901/15/WS5c3d2bb0a3106c65c34e46e2.html>. Also see: *China Releases National Automatic Vehicle Road Testing Rules. The National Law Review 2018.* Available at: <https://www.natlawreview.com/article/iot-update-china-releases-national-automatic-vehicle-road-testing-rules>
13. *Japan enacts bill to allow use of smartphones under some circumstances in self-driving cars. The Japan Times 2019.* Available at: <https://www.japantimes.co.jp/news/2019/05/29/national/japan-enacts-bill-allow-use-smartphones-circumstances-self-driving-cars/#.XR5b-ehKhPY>. Also see: *Japan edges closer towards brave new world of self-driving cars but hard questions remain. South China Morning Post 2019.* Available at: <https://www.scmp.com/news/asia/east-asia/article/2180828/japan-edges-closer-towards-brave-new-world-self-driving-cars>
14. *Ontario's Automated Vehicle Pilot Program. Ontario Ministry of Transportation 2019.* Available at: www.mto.gov.on.ca/english/vehicles/automated-vehicles.shtml.
15. *Corporate Truck Platooning Pilot Program. Ontario Ministry of Transportation 2019.* Available at: <http://www.mto.gov.on.ca/english/trucks/cooperative-truck-platooning.shtml>
16. *Harnessing the cybersecurity opportunity for growth. Ontario Centres of Excellence 2016.* Available at: https://www.oce-ontario.org/docs/default-source/publications/final_oce_tfsa_cyber-innovation-report_v6-2.pdf?sfvrsn=2
17. *Global Automotive Cybersecurity Report. Upstream Security 2019.* Available at: <https://industrytoday.com/wp-content/uploads/2018/12/Upstream-Security-Global-Automotive-Cybersecurity-Report-2019.pdf>
18. *Uber and Waymo Settle Trade Secrets Suit Over Driverless Cars. The New York Times 2018.* Available at: <https://www.nytimes.com/2018/02/09/technology/uber-waymo-lawsuit-driverless.html>

Endnotes



19. *Deloitte Global Automotive Consumer Survey (Canadian Data)*. Deloitte 2019. Available at: <https://www2.deloitte.com/us/en/pages/manufacturing/articles/automotive-trends-millennials-consumer-study.html>
20. *Making smart cities cybersecure: Ways to address distinct risks in an increasingly connected urban future*. Deloitte 2019. Available at: <https://www2.deloitte.com/insights/us/en/focus/smart-city/making-smart-cities-cyber-secure.html>
21. *Securing the networked vehicle: The Threat Landscape*. Deloitte 2016. Summary available (and full report available upon request) at: <https://www.linkedin.com/pulse/securing-networked-vehicle-nick-deshpande>
22. *Preparing for the future of transportation*. WSP 2018. Available at: <http://www.wsp.com/-/media/Sector/US/Document/Summary-of-USDOTs-Automated-Vehicles-30.pdf>
23. *The Key Principles of Cyber Security for Connected and Automated Vehicles*. UK Government 2018. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/661135/cyber-security-connected-automated-vehicles-key-principles.pdf
24. *The fundamental principles of automotive cybersecurity*. British Standards Institution (BSI) 2018. Available for purchase at: https://shop.bsigroup.com/ProductDetail/?pid=00000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114
25. *How the Land Transport Authority's (LTA's) Technical Reference 68 fueled Singapore's autonomous vehicle agenda*. Techwire Asia 2019. Available at: <https://techwireasia.com/2019/03/how-the-lta-tr68-fuelled-singapores-autonomous-vehicle-agenda>
26. *The Country Best Prepared for Autonomous Vehicles*. Forbes 2018. Available at <https://www.forbes.com/sites/niallmccarthy/2018/10/23/the-countries-best-prepared-for-autonomous-vehicles-infographic/#1a68dc4c3df2>
27. *How Singapore is driving the development of Autonomous Vehicles*. CIO - IDG Communications 2019. Available at: <https://www.cio.com/article/3294207/how-singapore-is-driving-the-development-of-autonomous-vehicles.html>
28. *Singapore develops provisional national standards to guide development of fully autonomous vehicles*. Land Transport Authority 2019. Available at: <https://www.lta.gov.sg/apps/news/page.aspx?c=2&id=8ea02b69-4505-45ff-8dca-7b094a7954f9>
29. *The UK Connected and Automated Mobility Roadmap to 2030*. Zenzic UK 2019. Available at: <https://triangle.ifourhosting.co.uk/what-we-do/uk-connected-and-automated-mobility-roadmap>
30. *H.R.3388 - SELF DRIVE Act, 115th Congress. 2017-2018. (Passed by the U.S. House of Representatives, not yet passed by the Senate. Latest Action: Received in the Senate; read twice and referred to the Committee on Commerce, Science, and Transportation)*. Available at: <https://www.congress.gov/bill/115th-congress/house-bill/3388/text>.
31. *Autonomous vehicles | Self driving vehicles enacted legislations*. National Conference of State Legislation 2019. Available at: <http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx>
32. *Draft proposal to introduce a Regulation on Cyber Security*. United Nations Economic and Social Council 2018. Available at: <https://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-02e.pdf>. For the framework, also see: *Framework document on automated/autonomous vehicles*. 2019. Available at: <https://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29/WP29-177-19e.pdf>
33. *The PROMETHEUS project launched in 1986: Pioneering autonomous driving*. Daimler AG 2016. Available at: <https://media.daimler.com/marsMediaSite/en/instance/ko/The-PROMETHEUS-project-launched-in-1986-Pioneering-autonomous-driving.xhtml?oid=13744534>
34. *Honda to invest \$2.75 billion in GM's self-driving car unit*. Reuters 2018. Available at: <https://www.reuters.com/article/us-gm-autonomous/honda-to-invest-2-75-billion-in-gms-self-driving-car-unit-idUSKCN1MD1GW>
35. *Waymo expands autonomous driving partnership with Fiat Chrysler*. TechCrunch 2018. Available at: <https://techcrunch.com/2018/05/31/waymo-expands-autonomous-driving-partnership-with-fiat-chrysler>
36. *Uber self-driving tech group receives \$1B investment led by Toyota*. CNET 2019. Available at: <https://www.cnet.com/roadshow/news/uber-1bn-investment-self-driving-cars-toyota-denso>
37. *BMW and Daimler team up on cars of the future to fend off Silicon Valley*. CNN 2019. Available at: <https://www.cnn.com/2019/02/28/business/bmw-daimler-driverless-cars/index.html>
38. *The Threat 3-D Printing Could Pose To Global Security*. Forbes 2018. Available at: <https://www.forbes.com/sites/jenniferjohnson/2018/05/29/does-3-d-printing-present-a-threat-to-global-security/#155eb4ad2535>
39. *Driving Prosperity: The future of Ontario's Automotive Sector*. Government of Ontario 2019. Available at: <https://news.ontario.ca/medg/en/2019/02/driving-prosperity-the-future-of-ontarios-automotive-sector.html>
40. *The London Office For Rapid Cybersecurity Advancement (LORCA) 2019*. Available at: <https://www.lorca.co.uk/what-we-do/>
41. *Angoka 2019*. Available at: <http://angoka.io/>
42. *Argus 2019*. Available at: <https://argus-sec.com/argus-solution-suites/>
43. *Dellfer 2019*. Available at: <https://dellfer.com/>
44. *ISARA 2019*. Available at: <https://www.isara.com/>



45. *Regional Technology Development Sites. Autonomous Vehicle Innovation Networks 2019.* Available at: <https://www.avinhub.ca/regional-technology-development-sites/#el-531e46b1>
46. *Ryerson University Announces \$30 Million in Public and Private Support for Rogers Cybersecure Catalyst. Ryerson University 2019.* Available at: <https://www.ryerson.ca/cybersecure-catalyst/news/rogers-cybersecure-catalyst/>
47. *Autonomous Vehicle Innovation Centre (AVIC). Blackberry QNX 2019.* Available at: <http://blackberry.qnx.com/en/blackberry-qnx-autonomous-vehicle-innovation-centre>
48. *Blackberry QNX and Blackberry Certicom 2019.* Available at: <https://blackberry.qnx.com/en> and <https://blackberry.certicom.com/>
49. *CloudGRC Inc. 2019.* Available at: <https://www.cloud-grc.com/automotive-industry/>
50. *ESCRYPT 2019.* Available at: <https://www.escrypt.com/en/industries/automotive-security> and <https://www.escrypt.com/en/news-events/transport-canada-contract>
51. *EZFleet - Fleet management solutions for autonomous vehicles. Easymile 2019.* Available at: <https://easymile.com/solutions-easymile/ezfleet-by-easymile>
52. *Bigchaindb 2019.* Available at: <https://www.bigchaindb.com/features/>
53. *SAFERIDE technologies 2019.* Available at: <https://saferide.io/>
54. *Centri 2019.* Available at: <https://www.centritechnology.com/company-about-centri/>
55. *ARXAN 2019.* Available at: <https://www.arxan.com/>
56. *NVIDIA 2019.* Available at: <https://www.nvidia.com/en-us/about-nvidia/>
57. *Mitsubishi 2019.* Available at: <https://www.mitsubishi-motors.com/en/index.html>
58. *Trillium 2019.* Available at: <https://trilliumsecure.com/solutions/>
59. *AT&T Ventures into the Connected Car Industry in Mexico. The Fast Mode 2018.* Available at: <https://www.thefastmode.com/services-and-innovations/13148-at-t-ventures-into-the-connected-car-industry-in-mexico>
60. *Jooycar 2019.* Available at: <https://jooycar.com/>
61. *SOS LAB Secures \$6M in Series A Funding Round. Business Wire 2018.* Available at: <https://www.businesswire.com/news/home/20181005005114/en/SOS-LAB-Secures-6M-Series-Funding>
62. *CUBE NEWS – Monthly Report March 2019. Cube Intelligence 2019.* Available at: <https://blog.cubeint.io/2019/03/cube-news-monthly-report-march-2019.html>
63. *Quantoz 2019.* Available at: <https://quantoz.com/>

Key terms



- **AV** – Autonomous Vehicle or Automated Vehicle.
 - Other terms commonly used to refer to AV include: self-driving cars, Highly Automated Vehicles (HAVs), Automated Driving Systems (ADS).
- **Botnets** – A type of malware that takes control of a host device and uses it to preform attacks, send spam, steal data, etc.
- **CAV** – Connected and Autonomous Vehicle.
- **Distributed Denial of Service (DDOS)** – A large number of internet requests, usually sent by a botnet, which are intended to overwhelm a system to bring the website or system offline.
- **Insider threats** – An inside user account of the organization (employee, contractor, etc.) who performs an attack, either by the owner of the account or due to the account being compromised by an external attacker.
- **IoT** – Internet of Things.
- **LIDAR** – Light Detection and Ranging; A remote sensing method that uses light to measure distances
- **Malware** – Any type of malicious software.
- **Malware outbreak** – Malware on several computers or systems within an organization.
- **OEM** – Original Equipment Manufacturer.
- **Phishing** – An attack where the attacker attempts to convince an employee that a communication (email, phone call, etc.) comes from a valid source and to follow instructions given.
- **Ransomware** – A type of malware that encrypts data on a device and demands a ransom for the decryption key.
- **Roadside unit (RSU)** – Roadside units provide wireless communications from roadside infrastructure to connected vehicle systems. RSUs engage with On-Board Units (OBUs) or On-Board Diagnostics (OBDs) of vehicles to acquire information such as time, speed and location to assist with events such as crash avoidance.
- **SAE** – Society of Automotive Engineers.
- **Security convergence** – The combination of cybersecurity and physical security.
- **Spoofing** – A type of attack (usually over the network) where a user, system or a connection is masqueraded by falsifying data to get an illegitimate advantage.
- **TCU** – A Telematics Control Unit is an embedded system within a vehicle that transmits and interprets data within the vehicle or to and from servers located externally to the vehicle, for example, from OEMs to distribute over-the-air (OTA) software updates.
- **Threat landscape** – Identified threats, based on trends across the ecosystem.
- **V2I** – Vehicle to infrastructure communication.
- **V2V** – Vehicle to vehicle communication.
- **V2X** – Vehicle to everything communication.
- **WEF** – World Economic Forum.

Appendix

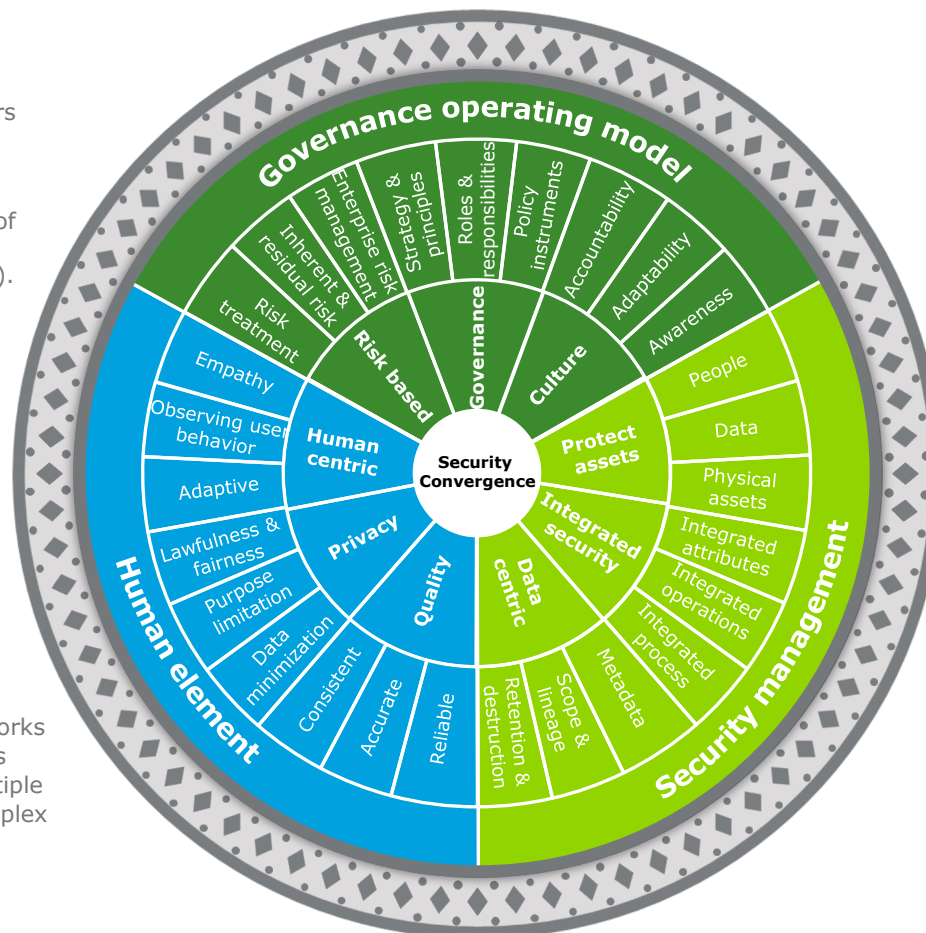
● Security Convergence and Privacy by Design frameworks	28
● Security convergence opportunity for CAV testing facilities	31
● Key use cases: Emerging initiatives in the CAV ecosystem	32
● Global CAV cybersecurity solution developments	34

A security convergence framework for the CAV ecosystem

Deloitte's comprehensive framework – security convergence, cybersecurity and privacy by design – can be used to understand the various aspects of physical security, cybersecurity and privacy, across the CAV ecosystem.

The Need for a Convergence Cybersecurity Framework

The complex CAV ecosystem requires a framework that considers **Security Convergence** (the merging of physical and cybersecurity) and **Privacy by Design**, as well as the key pillars of a robust cybersecurity strategy framework (such as Deloitte's CSF).



It allows for the consideration of the combination of physical and digital realms impacting the CAV, as well as the organization's own cybersecurity strategy – which also needs to be robust in order to ensure the privacy and cybersecurity safeguards are designed from the outset.

The combination of these frameworks allows for the analysis of key risks across the CAV supply chain, multiple communication channels and complex data lifecycles.

Deloitte's **Security Convergence shield** provides a holistic set of nine principles across three domains to guide and assess an organization's maturity and capabilities in their journey towards convergence.

A security convergence framework for the CAV ecosystem—

A detailed description of the components in Deloitte's Security Convergence framework:



The **human element** focuses on the ultimate providers and consumers of services – people, to ensure the design is human-centric, respects their privacy and ensures the quality of the data driving the decisions is maintained.

Human-centric

Making sure solutions, designs, and processes are end user intuitive and adaptive is crucial for increased participation and adoption of a successful converged approach

Privacy

Having *Privacy by Design* is necessary to gain and ensure the trust of the people sharing their data as well as meeting regulatory requirements such as GDPR

Quality

Decisions are only as good as the data supporting them and hence it is vital to make sure the data driving the algorithms is consistent, reliable and accurate



Security management relates to the protection of the crown jewels using a connected and data-centric lens along with having an integrated security approach.

Data-centric

In order to ensure correctness and meaningful results, data from cyber-physical systems needs to be managed efficiently throughout its lifecycle with the help of robust metadata management

Integrated security

Ensure integration of various security and related functions including IT, privacy, legal, HR and business units at the people, process and technology levels to ensure seamless flow of information

Protect assets

Organizations need to protect all their crown jewels – people, data and assets – in a secure, vigilant and resilient manner to ensure successful delivery of critical services and operations



Governance operating model provides guidelines for establishing a collaborative governance based on the risk appetite and imbibing a convergence culture to transform the security domain from a cost center to a value center.

Culture

Imbibing a culture of an adaptive environment where each individual takes accountability and are empowered by means of appropriate training and awareness

Governance

Having a governance model in place guided by a strategic vision and well-defined roles and responsibilities enables the organization in effectively managing converged risks

Risk-based

Prioritizing resource allocations and actions based on the risk environment is the foundation of an effective enterprise risk management program

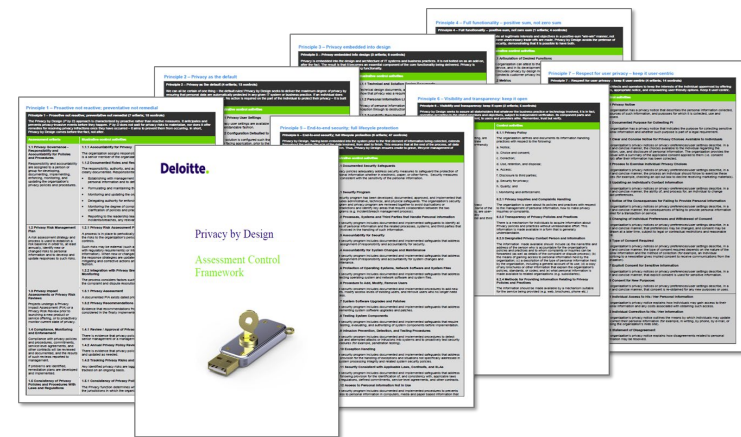
The Privacy by Design framework



The 7 Privacy by Design principles can be incorporated into the CAV design, development, and deployment process to keep privacy at the forefront of CAV ecosystem decision-making.

7 Foundational Privacy by Design Principles

- 1 Proactive not reactive: preventative not remedial**
- 2 Privacy as the default setting**
- 3 Privacy embedded into design**
- 4 Full functionality: positive-sum, not zero-sum**
- 5 End-to-end security: full lifecycle protection**
- 6 Visibility and transparency: keep it open**
- 7 Respect for user privacy: keep it user-centric**



Harmonized privacy control framework

Deloitte, together with Ryerson University's Privacy by Design Centre for Excellence, has developed a Privacy by Design control framework based on the Generally Accepted Privacy Principles (GAPP) as the foundation, and incorporating Canadian and international privacy legal requirements (e.g., PIPEDA, GDPR), industry best practices and privacy standards (CSA Model Code, ISO/IEC 27001/2, ISO/IEC 27018, ENISA), and regulatory guidance.

Security convergence opportunity for CAV testing facilities

Vehicle test centres' core capabilities and the potential inclusion of cybersecurity testing for CAVs

Vehicle safety testing centers typically provide an evaluation of:

1 | Structural durability

2 | Various life-cycle tests

[For example, how long a particular component of the vehicle lasts and various stress points of a component's use]

3 | Climatic conditions

With connected and autonomous vehicles, cyber risks are combined with risks in the physical environment. Adding cybersecurity components to current CAV testing centre capabilities can establish centres for convergence security testing – facilities that can be used for identifying vulnerabilities across both physical and cybersecurity realms. Below are recommended cybersecurity testing activities that could be added to existing aspects of physical safety and security testing conducted within CAV testing facilities.

A | Hardware

[in combination with 'structural durability']

Non-volatile memory and firmware can be extracted, analyzed, and modified. Safeguards should be tested to prevent extraction.

EXAMPLE | Onboard memory

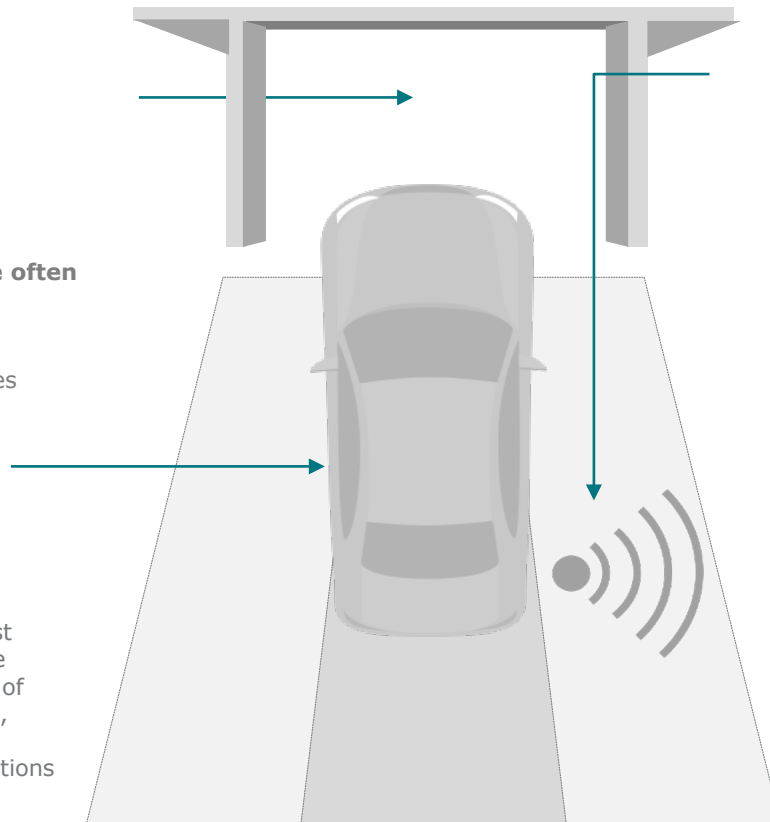
Non volatile memory content are often susceptible to extraction:

- Contents are rarely encrypted
- Can store hard coded credentials
- Can be modified (security features disabled)

B | Software

[in combination with 'life-cycle testing']

Software used to enable CAV functionality can be vulnerable to attacks, and should be tested against possible cyber threats – both remote and near or inside the car. Features of CAVs that provide convenience (e.g., remote start) should be tested for vulnerabilities that may aid cyber actions such as 'Man in the Middle' attacks.



C | Vehicle communications

[in combination of 'life-cycle testing']

Vulnerabilities across V2X communications (e.g., vehicle to infrastructure, individuals, or other vehicles) should be tested. Physical access to the vehicle communication bus can be the equivalent of root access on a server, so both physical and cyber threats must be considered.

EXAMPLE | Message spoofing

Unencrypted and unauthenticated messages are commonplace:

- Susceptible to replay attacks
- Susceptible to spoofing or modification
- Critical sensor data such as object detection could be manipulated



Key use cases: Emerging cybersecurity initiatives in the CAV ecosystem [International]

Start-ups often focus on one key CAV threat vector and develop one or more impactful technologies. Start-ups may go to market independently or in collaboration with another organization (for example, with government, manufacturers, and telecoms).

Collaboration with government

LORCA

CASE STUDY 1
Innovator's hub
[United Kingdom]

London Office For Rapid Cybersecurity Advancement (LORCA) 12-month innovation program:

*LORCA is an Innovation Centre funded by the government to support startup companies working on innovations. These startups are on a program, where they receive support to provide solutions to cybersecurity challenges for the automotive industry and other industries. Angoka is a participant in the LORCA innovation program.*⁴⁰



Cybersecurity CAV technology company

ANGOKA

CASE STUDY 2
ANGOKA
[United Kingdom]

Cybersecurity technology designed for the CAV:

*Angoka is developing S-CAN: a future-proof hardware solution for securing network communications. Originally developed for the CAN bus, which is used widely in the automotive sector for in-vehicle communications between ECUs, the technology is also portable to other types of networks such as industrial control systems and various other forms of machine-to-machine (M2M) communications.*⁴¹



Collaboration with a manufacturing company

ARGUS
CYBER SECURITY

CASE STUDY 3
Argus cyber security
[Israel]

Go-to-market approach with a manufacturer:

*German firm Continental AG acquires Argus. Argus collaborates with Continental – the organization jointly launched a technology for delivering over-the-air vehicle software updates with Continental subsidiary Elektrobit. Argus would now become part of Elektrobit and would continue to engage in commercial relations with all automotive suppliers globally.*⁴²



Collaboration with telecom company

 **dellfer**

CASE STUDY 4
Dellfer
[United States]

Go-to-market approach with a telecom provider:

*Partnered with DENSO (world's 2nd largest mobility provider) for Joint Development Agreement (JDA) to bring ZeroDayGuard 1.0 to market. ZeroDayGuard is Dellfer's IoT cybersecurity solution that prevents zero-day cyberattacks on IoT devices through built-in code execution protection. It is enabled with one operation in the development of IoT device code, and subsequently can instantaneously detect root cause hacks and cyberattacks remotely in the cloud.*⁴³



Key use cases: Emerging cybersecurity initiatives in the CAV ecosystem [Canada]

Start-ups in Ontario are engaging in research and developing technologies. Some start-ups and innovation hubs focus on technologies within the CAV ecosystem.

Cybersecurity CAV technology company



CASE STUDY 5

ISARA

[Kitchener Waterloo, Canada]

Cybersecurity technology designed for the CAV:

ISARA, with expertise including cryptographers, researchers, developers, and security industry veterans, work to create production-ready cybersecurity solutions, with optimized encryption that can be seamlessly integrated into existing infrastructure, to remain secure into the post-quantum age.

ISARA offers two solutions

The ISARA Radiate™ Quantum-safe Toolkit is the first complete security solution to offer a production-ready, easy-to-use implementation of quantum-safe algorithms and integration tools built for developers.

ISARA Catalyst™ agile technologies enable you to introduce crypto-agility into your existing systems as a risk-free, confident step towards quantum-safe security today.⁴⁴

Regional Technology Development Sites



CASE STUDY 6

AVIN RTDSs

[Ontario, Canada]

Innovation and development sites:

The Autonomous Vehicle Innovation Network (AVIN) brings together industry, academia, and governments to capitalize on the economic opportunities of Connected and Autonomous Vehicles (CAVs), while supporting the province's transportation systems and infrastructure in adapting to these emerging technologies.

The Regional Technology Development Sites include the creation of locations that enable Ontario-based small- and medium-sized enterprises (SMEs) to develop, prototype, and validate new technologies, access specialized equipment (hardware and software), and obtain business and technical advice.

Each RTDS has a unique specialization; however, all the six RTDSs consider CAV cybersecurity as an integrated part of their own specializations due to the broad and significant impact of cybersecurity on the whole CAV system and underlying technologies.⁴⁵

Global CAV cybersecurity solution developments



Jurisdiction	Organization	Description of CAV Cybersecurity Innovation Cybersecurity innovation stage: Ideas [I], Development [D], and in the Market [M]*	*Stage
Canada	ISARA	ISARA expertise includes cryptographers, researchers, developers, and security industry veterans, work to create production-ready cybersecurity solutions, with optimized encryption that can be seamlessly integrated into existing infrastructure, to remain secure into the post-quantum age. ⁴⁴	D
	Rogers Cybersecure Catalyst (Ryerson University)	Ryerson University's Rogers Cybersecure Catalyst program is a new national centre for innovation and collaboration in cybersecurity. This program is aimed at growing cybersecurity in Canadian organizations through training and skills advancement, research and development, educating small businesses on cyber threats and how to address them, certifications, and the build of a commercial accelerator and a simulated security operations centre located in downtown Brampton. ⁴⁶	I, D
	BlackBerry	BlackBerry's Autonomous Vehicle Innovation Centre (AVIC) was created to advance technology innovation for CAVs, independently as well as in collaboration with private and public sector organizations and research institutes. ⁴⁷ BlackBerry has a number of connected car security solutions and services currently in the market, including BlackBerry Certicom and BlackBerry QNX software solutions supporting CAVs. ⁴⁸	I, D, M
	CloudGRC	CloudGRC Inc. is a leader in automotive cybersecurity that provides the expertise and the experience to build an effective risk-based cybersecurity program for enterprise organizations that are involved in the production and operation of CAVs. This includes building an enterprise cybersecurity program, cybersecurity strategy, threat and risk assessment, penetration testing & vulnerability assessment, continuous identity assurance and vehicle monitoring. CloudGRC also provides training and workshops in the field of automotive cybersecurity. ⁴⁹	I, D, M
	ESCRYPT Canada	Transport Canada recently awarded a contract valued at up to \$1.3 million to ESCRYPT to advance the development of a Canadian Security Credential Management System (SCMS) for connected vehicles. The SCMS will help ensure that connected vehicle communications are secure and can be trusted. The SCMS incorporates privacy-by-design principles and enables communication without revealing personal information about the vehicle or the driver. As part of the contract, ESCRYPT will be responsible for developing Canadian requirements for the system and recommending an operational model for how the technology may be deployed in Canada. ⁵⁰	I, D, M
Germany	ESCRYPT	CycurHSM product is an innovative and flexible HSM security firmware that ensures secure boot of the ECU, secure in-vehicle communication, ECU component protection and secure flashing. ⁵⁰	I, D, M
	EasyMile	Vehicles are equipped with a Black Box module. The module records the raw data from the various sensors exchanged between the vehicles' hardware and software parts. In case of a critical event, all data is recorded prior and after the event to help understand and diagnose the event. Metrics include: Quality metrics (sensors, location and route monitoring), position, assignments sent to the vehicle by the supervision system, usage statistics. EZFleet services specific to transportation vehicles: EZFleet is the electronic brain behind a fleet of driverless vehicles. Flexible and modular, it enables organizations to adapt their fleet according to different operating scenarios and needs. ⁵¹	D
	Bigchain DB	Allows developers and enterprise to deploy Blockchain proof-of-concepts, platforms and applications with a scalable Blockchain data-base. Rather than trying to scale up Blockchain technology, starts with a distributed database and then adds Blockchain characteristics – decentralized control, immutability and the ability to create and transfer assets. ⁵²	I

Global CAV cybersecurity solution developments



Jurisdiction	Organization	Description of CAV Cybersecurity Innovation Cybersecurity innovation stage: Ideas [I], Development [D], and in the Market [M]*	*Stage
Israel, Tel Aviv and Ramla	SafeRide Technologies	Multi-layer deterministic and heuristic anomaly detection and threat prevention solutions for connected cars, SafeRide Technologies recently augmented its suite of security solutions with advanced AI technology. vXRay, a behavioral profiling and anomaly detection solution for Security Operation Centers (SOCs) in connected cars. Without any dependencies or prior knowledge of the vehicle's behavioral protocols, vXRay uses machine learning to create an individual behavioral profile, which the system uses to identify abnormal behavior and alert the car's SOC. ⁵³	I, D, M
United States	Centri	Installs chips and mobile apps to protect automobile sensors and data. Requires no internet connection; connects trusted devices with identity management technology. ⁵⁴	D, M
	Arxan technologies	Binary level code obfuscation, data encryption and real-time cyber threat alerts. ⁵⁵	D, M
	NVIDIA	AI-powered data processors and chips; software and cloud-based technologies help autonomous vehicles securely learn and relay driving data. Deep learning systems have been used by Tesla, Mercedes-Benz, Audi, Toyota and Volkswagen to power and protect self-driving vehicles. ⁵⁶	I, D
Japan	Mitsubishi	Threat detection technologies. Encryption in cloud environments: "attribute-based encryption" restricts access rights to the ciphertext. ⁵⁷	D
	Trillium Inc.	Secures all three key 'cyber-threat domains' in the car with a software-based approach compatible with any architecture or operating system. Security as a Service (SaaS) via real-time-update platforms that automakers or insurers will on-sell to car owners. Expertise in testing, 'SecureCAR' and 'SecureIoT' and expand in-vehicle implementation and testing of cyber-security retrofits on current-model connected vehicles. ⁵⁸	D
Mexico	AT&T partners with KIA	MyKIA + is a mobile application developed by KIA. Via its recovery service, Find My Kia, drivers are provided an optional device that not only tracks and locates the car at any time, but also delimits, virtually, its travel area. Services will be provided via the AT&T Control Center platform where the IoT solutions are administered. RESSER, the satellite tracking company that provides the vehicle recovery service will be working with the control center to keep tab of the location of the cars at all times, thus speeding up search processes. ⁵⁹	D
	Jooycar	Obtain real time data from vehicles and drivers while using Artificial Intelligence techniques in order to offer connected insurance and smart services with added value. ⁶⁰	D
South Korea	SOS LAB	Technology company that manufactures LiDAR sensor products, scanning solutions for autonomous vehicles. ⁶¹	D
	Cube Intelligence IO [CUBE.IO]	With the use of AI, protects against malicious attacks on hacking for autonomous cars and connected cars using hash codes that form the core of block chain technology and block chains. Cube blocks these attacks using its own developed Synapse. To grow local innovation, Cube AI participated in 'Open Innovation Program' for innovative technology/product startups sponsored by Volkswagen Korea. ⁶²	I, D
Netherlands	Quantoz	Innovative Blockchain technology application incubator. Quasar, the Quantoz digital cash solution provides the infrastructure for instant payment and transaction settlement between enterprises, consumers and the Internet of Things, compliant with regulations while respecting the user's privacy. ⁶³	I, M

About the Autonomous Vehicle Innovation Network

The Autonomous Vehicle Innovation Network (AVIN) is an initiative by the Government of Ontario and delivered by the Ontario Centres of Excellence on their behalf. AVIN is ensuring that Ontario remains a leader in the automotive and transportation sector by capturing the economic opportunities presented by connected and autonomous vehicle and mobility solutions, while supporting Ontario to lead in readiness, adoption and deployment of these technologies.

About Ontario Centres of Excellence

Ontario Centres of Excellence (OCE) Inc. drives the commercialization of cutting-edge research across key market sectors to build the economy of tomorrow and secure Ontario's global competitiveness. In doing this, OCE fosters the training and development of the next generation of innovators and entrepreneurs and is a key partner with Ontario's industry, universities, colleges, research hospitals, investors, and governments.

About the APMA

The Automotive Parts Manufacturers' Association (APMA) of Canada is a national association representing OEM producers of parts, equipment, tools, supplies, advanced technology, and services for the worldwide automotive industry. Founded in 1952, its members account for 90% of independent parts production in Canada. The Association's fundamental objective is to promote the original equipment (O.E.) automotive supply manufacturing industry both domestically and internationally. In addition to advocacy, the APMA also provides its members business development solutions as well as guidance and assistance on modernizing their operations to suit the needs of Industry 4.0. and CASE (Connected, Automated, Shared and Electric) integration.

About Deloitte

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

About this publication

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.