Information and Communications Technology Council

Developing Cyber Talent for Canadian Road Authorities

Report prepared for Transport Canada

2019

PREFACE

The Information and Communications Technology Council (ICTC) is a not-for-profit national centre of expertise for the digital economy. With over 25 years of experience delivering evidence-based research, innovative talent solutions, and practical policy advice, ICTC's goal is to support Canada's digital advantage in a global economy via fostering globally competitive Canadian industries empowered by a talented and diverse digital workforce.

This report was funded by Transport Canada.

Transport Canada Transports Canada

The authors made all reasonable efforts to ensure accuracy and fair reflection of the diverse perspectives gathered during consultations in compiling the document. The opinions and interpretations in this publication are those of the authors and do not necessarily reflect those of the Government of Canada.

To cite this report:

Ye, Z., Donaldson, K., Davidson, R. (2017). *Developing Cyber Talent for Canadian Road Authorities*. Information and Communications Technology Council (ICTC). Ottawa, Ontario.

Elaborated and written by Zhenzhen Ye (Senior Economist and Data Analyst, Research & Policy), Kadeem Donaldson (Economist, Research & Policy), Rob Davidson (Manager of Data Analytics and Research, Research & Policy), with generous support from Alexandra Cutean (Senior Director, Research & Policy).

ACKNOWLEDGEMENT

ICTC would like to thank everyone who made this report possible. Specifically, the contributions made by those interviewed during the production of this report are greatly appreciated. We would like to acknowledge the following individuals and their contributions:

- Carl Clayton, Global Technology in Infrastructure Lead (IBI Group)
- Brigid McGoran Canil, Acting Director, Electrical and ITS Engineering (BC Ministry of Transportation and Infrastructure)
- Graeme Cross, Traffic Signals Team Leader (City of Surrey)
- Mark Dietelbach, IT Architect (City of Surrey)
- Siva R. K. Narla, Senior Director, Transportation Technology (Institute of Transportation Engineers)
- Pino Porciello, Director - Product Management and Strategic Marketing (ESCRYPT)
- Nadia Diakun-Thibault, Senior Aviation Security Policy Officer (blockchain and identity) (Transport Canada)

CONTENTS

GLOSSARY

ATIS: Advanced Traveler Information System - These systems consist of a wide variety of communication devices such as cell phones, televisions, radio, and the Internet, all of which helps commuters make informed travel decisions with regards to departure time, and the most convenient routes and modes of transportation

ATMS: Advanced Traffic Management System - Technologies that are used mainly by road traffic authorities as a means to monitor and control traffic flow. This is done by using real-time information to intervene and adjust controls like traffic signals in order to optimize the movement of vehicles.

APTS: Advanced Public Transportation System -These apply transportation management and information technologies to public transit systems to increase the operational efficiency of all modes of public transportation, increasing ridership, and improving the overall reliability of the transport system

AVs: Automated vehicles -Vehicles that use a combination of sensors, cameras, radar and artificial intelligence (AI) to travel between destinations without a human operator.

CEH: Certified Ethical Hacker (offered by EC-Council)

CI: Critical Infrastructure

CISA: Certified Information Systems Auditor (offered by ISACA)

CISM: Certified Information Security Manager (offered by ISACA)

CISSP: Certified Information Systems Security Professional (offered by (ISC)^2).

CSA: The CSA Group, formerly the Canadian Standards Association

CVs: Connected vehicles. Vehicles that use any of a number of different communication technologies to communicate with the driver, other cars on the road (vehicle-to-vehicle [V2V]), roadside infrastructure (vehicle-to-infrastructure [V2I]), and the “cloud” [V2C]

EMS: Emergency Management System - These systems consists of a number of different safety oriented

GIAC: Global Information Assurance Certification (cybersecurity certifications)

ICS: Industrial Control Systems - is a general term that encompasses several types of control systems and associated instrumentation used for industrial process control

ICT: Information and Communications Technology

ISO 27000: Information technology -- Security techniques -- Information security management systems

ITE: The Institute of Transportation Engineers

ITS: Intelligent Transportation Systems - These are systems that incorporate the use of advanced and emerging technologies such as computers, sensors, controls communications and electronic devices in the transportation infrastructure and that which helps to improve the overall safety and efficiency of the transport network

KII: Key Informational Interviews

LPT: Licensed Penetration Tester (offered by EC-Council)

NIST: (U.S.) National Institute of Standards and Technology

OT: Operational Technology. In the context of this report, OT refers to equipment and systems that are part of ITS (e.g. cameras, traffic signals)

OTCF: Operational Technology Cybersecurity Framework - An OT system framework that maps all OT assets and infrastructure from a cybersecurity perspective

EXECUTIVE SUMMARY

With an extensive road network and a two-lane equivalent length covering a little over one million kilometers, Canada places 7th in the world in terms of size. Canadian road authorities face a number of unique challenges due to factors including the country's vast and varying geography and sometimes harsh climate, the high degree of urbanization, and the significant rate of cross border trade with the U.S. Other challenges are similar to that of many modern economies around the world, such as the increased demand for more efficient and expansive transportation systems, as a result of traffic and population growth.

To begin responding to such challenges, Canadian road authorities have employed and adopted robust Information and Communications Technologies (ICT), Operational Technologies (OT) and Industrial Control Systems (ICS) to provide improved safety and efficiency to road users. These are collectively referred to as Intelligent Transportation Systems (ITS). Today's road transportation system is a combination of legacy technology like ramp metering systems and networked traffic signals and newer developments like Advanced Traffic Management System (ATMS), Bluetooth detection, high definition video and data analytics. While traditionally, legacy systems were closed, not wirelessly accessible, and electro-mechanical rather than computerized, increased connectivity capabilities via the Internet have brought these systems online. In turn, this has created new considerations related to cybersecurity practices and procedures. Because of the critical role that road transportation networks play for our country and our economy, we need to increasingly focus on ensuring that this very infrastructure is reliable and effective – and with the increasing permeation of digital technology across our economy, questions of cybersecurity and digital needs pertaining to these systems must be brought to the forefront.

The objective of this study is to identify the cybersecurity-related skills needed by Canadian road authorities to deploy, maintain, and protect road infrastructure systems. Our research and consultations with key leaders in this space uncovered significant gaps in Canada's road transportation sector when it comes to building a sufficient and skilled cybersecurity talent pipeline. Both the availability and skill level of cybersecurity talent are important considerations, as this talent will be paramount to ensuring safety, effectiveness, and reliability of road infrastructure – particularly as advancements in connected and automated vehicle technologies become an everyday reality. At the same time, the establishment of road cybersecurity frameworks or standard protocols is essential. Our consultations with road authorities suggests these do not currently exist, due to a lack of cybersecurity awareness regarding potential risks, and a lack of transportation-specific cybersecurity training programs. Discoveries like these accentuate the need for transportation authorities to focus on cybersecurity.

Through consultations with industry experts based in the U.S. and Canada, complemented with comprehensive secondary research, ICTC suggests that Canadian road authorities develop an OT cybersecurity framework, a cybersecurity risk management plan and a cybersecurity protocol for legacy systems and ITS integration. A lack of adequately skilled talent in this space also indicates the need to build a cybersecurity skill development pipeline. These pathways can be forged by taking steps to partner with universities, colleges and professional development institutions in order to provide industry-specific cybersecurity training for OT professionals. Other angles can include the identification of trustworthy consulting firms that can serve as industry experts and training authorities as needed.

Taking action to develop a robust and effective system of cybersecurity practices and policies; while also developing, supporting and underlining the need for skilled cyber-talent with competencies specific to road infrastructure is essential. Only when this is addressed will Canadian road authorities be better equipped to tackle today's challenges, and capitalize on technological change driving key developments like connected and automated vehicles, while continuing to safeguard the reliability of roadways in an increasingly digital world.

INTRODUCTION

Being the second largest country in the world, Canada needs a strong transportation network to support the functionality and continued development of our cities and communities. Transportation has and continues to play a crucial role in our societies, bolstering the movement of passengers and freight across the country and internationally. Moreover, growing by a compound annual growth rate (CAGR) of more than 3% over the last 5 years[1], in 2017 the economic contribution of the transportation and warehousing sector totaled 4.6% of all Canadian gross domestic product (GDP).

In addition to this significant economic contribution, transportation is also one of the ten Critical Infrastructure (CI) sectors in Canada. Public Safety Canada defines CI as the "[…] processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government."[2] Critical infrastructure is also identified as being either stand-alone or interconnected and interdependent within and across provincial and even national lines. This means that critical transportation infrastructure can be a railway network connecting Halifax and Truro in Nova Scotia; or Toronto with Ottawa. At the same time, it can also be the port of Vancouver, receiving international freight and cargo from around the world. These pieces of infrastructure are so important that "disruptions [of them] could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence."[3]

While "critical transportation infrastructure" can include anything from railway networks, to harbours, to airports among others, Canada's transportation system is primarily based on road transportation – this is for both passengers and freight. Canada has more than a million kilometres of (two-lane equivalent) roads, roughly 38,000 of which make up the National Highway System (NHS)[4]. The country is connected from the Pacific coast to the Atlantic and Arctic coasts through a network of highways anchored by the Trans-Canada Highway (TCH). Ontario and Québec have the busiest road border crossings, and in 2016, Ontario was responsible for more than 52%[5] of Canadian exports to the U.S. in 2016.

It is clear that robust and resilient transportation infrastructure is a central concern for Canada. Such infrastructure ensures not only the continued transit of goods, but it maintains our ability to stay connected within cities, regions and provinces, as well as with other nations. Because of the critical role that transportation networks play for Canada, a focus on safeguarding their reliability and adaptability in an increasingly digital world is essential; and cybersecurity must be a key consideration.

The overall objective of this paper is to identify the cybersecurity-related skills needed by Canadian road authorities to deploy, maintain, protect, and continually improve Canada's road infrastructure systems. This study explores approaches to talent development across several jurisdictions, and examines the ways in which Canadian areas of academic expertise in cybersecurity can be leveraged to develop talent specific to road authorities. Finally, the study provides insights into policies that can prove effective in maximizing critical skills for cybersecurity talent.

Part 1 of this report provides an overview of recent technological developments related to Intelligent Transport Systems (ITS), and their role in accelerating the demand for cybersecurity talent among Canadian road authorities.

Part 2 of this report offers an overview on the methods currently used by Canadian road authorities to acquire necessary cyber talent; and highlights the challenges associated with these tactics. This comes with insights regarding the knowledge, skillsets, and expertise needed by Canadian road authorities to ensure the security (both physical and cyber) of the transportation systems. Lastly, a

[1] Transportation in Canada 2017 https://www.tc.gc.ca/eng/policy/transportation-canada-2017.html#toc1
[2] Critical Infrastructure (Date modified:2018-05-22)https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx
[3] Ibid.
[4] Transportation in Canada 2011 https://www.tc.gc.ca/eng/policy/anre-menu-3021.htm
[5] Ontario-U.S. Trade Tops the Chart (Date Modified:2017-05-25) https://www.tradecommissioner.gc.ca/canadexport/0001535.aspx?lang=eng

summary of existing training resources for road authorities to develop cyber talent and improve cyber skills is provided.

Part 3 of this report examines weather or not Canadian road authorities have the necessary talent to meet the needs of evolving road transportation systems and infrastructure. This includes an analysis of essential cybersecurity knowledge, skillsets and expertise of cybersecurity professionals in the transportation sector.

Part 4 of this report provides an overview of cybersecurity-centred talent development approaches adopted by other jurisdictions (e.g. U.S., U.K., E.U., Australia). It also analyzes the potential applicability of these approaches in Canada.

Part 5 is the concluding section of this report, offering recommendations aimed at helping maximize the availability cybersecurity talent with critical skills for Canadian road authorities.

Part 1: Overview

1.1 Road authorities in Canada: Mandates and Responsibilities

In Canada, the majority of highways and local roads fall under the remit of the provinces, territories and municipalities. Their scope of responsibilities include the financing, planning, design, and delivering road works within their respective localities.[6] An overall breakdown shows that approximately 64% of all roadways[7] fall under the jurisdiction of municipalities, while provinces are responsible for roughly 16%. By comparison, the federal government is responsible for a mere 1%, and another 19% falls under the remit of private interests - the majority of which are constructed and maintained by private companies to gain access to natural resources such as forests, minerals etc. [8] Examples of resource roads are those which can be found in BC, accounting for over 620,000 kilometers of the road network in that province, and are used mainly by industrial vehicles operating in the forestry, mining, oil & gas and agriculture sectors.[9]

The provinces have overall oversight for the roads that fall under their jurisdictions, with operations belonging to the municipalities. For instance, in BC, The Ministry of Transportation and Infrastructure is responsible for planning transportation networks, providing services and infrastructure, developing and implementing transportation policies, and administering a number of transportation-related acts and regulations. However, when it comes to municipal jurisdiction, the City of Vancouver manages the road network within that locality, and in collaboration with TransLink[10], delivers a wide range of services and programs that cater to the transportation needs of Metro Vancouver residents.

The federal government, although being the "owner" of several important road infrastructure assets, has limited oversight when it comes to the active management of road and other modes of public transportation. However, through Transport Canada, the federal government plays an integral leadership role in ensuring that all parts of the transportation network operate effectively. This is achieved through collaboration with a number of important stakeholders including Indigenous peoples, private industry, provincial and territorial governments, and international partners.[11]

1.2 Opportunities and Challenges Resulting from Intelligent Transport Systems (ITS)

The development and adoption of ITS in various forms has had a transformative impact on the

[6] Transport Canada: https://www.tc.gc.ca/eng/policy/anre-menu-3021.htm
[7] Measured by total kilometers.
[8] Canada – National Report: Optimizing Road Infrastructure Investments and Accountability: http://www.tac-atc.ca/sites/tac-atc.ca/files/site/doc/resources/piarc-report.pdf
[9] Government of British Columbia: https://www2.gov.bc.ca/gov/content/industry/natural-resource-use/resource-roadsa
[10] Translink is the transit operator that manages and administers the transport system in the Metro Vancouver area in British Columbia.
[11] Transport Canada: https://www.tc.gc.ca/eng/aboutus-department-overview.htm

transportation landscape. ITS are predominantly integrated systems that incorporate the use of ICT and OT systems into transportation infrastructure. They perform tasks like assisting with the monitoring and management of traffic flow, and responding to traffic incidents. Key examples include the Advanced Traveler Information System (ATIS), the Advanced Traffic Management System (ATMS) the Advanced Public Transportation System (APTS), and the Emergency Management System (EMS). All of these are widely used around the world to address traffic and other road transportation needs.[12]

An Advanced Traveler Information System (ATIS) incorporates a wide variety of communication devices like cell phones, televisions, radio, and the Internet. It helps commuters make informed travel decisions with regard to departure time, and the most convenient routes and modes of transportation. The Advanced Traffic Management System (ATMS) is used mainly by road traffic authorities as a means to monitor and control traffic flow. This is done by using real-time information to intervene and adjust traffic signals in order to optimize the movement of vehicles. These systems usually consists of sensing, communications, and data-processing technologies, and are often deployed to alleviate traffic congestion.[13] The Advanced Public Transportation System (APTS) focuses on increasing the operational efficiency of all modes of public transportation to improve the overall reliability of the transport system.[14] Lastly, Emergency Management Systems (EMS) are considered to be one of the more recent developments in the area of ITS, and are primarily an integration of a number of different safety-oriented applications within the overall transportation infrastructure.[15] It provides effective assistance in emergency situations such as road accidents.

Cybersecurity Vulnerabilities Resulting from System Integration

The advancement and applications of ITS have effectively improved safety and efficiency to road users. They have also enabled road authorities to access real time data and control remote systems that enhance productivity and efficiency of road transportation networks. However, such efficiency and productivity gains are at a cost of increasing cybersecurity vulnerabilities resulting from the convergence of ICT and OT systems. Traditionally, OT networks and systems, such as Industrial Control Systems (ICS) or Supervisory Control and Data Acquisition (SCADA), have had a degree of physical separation from the ICT infrastructures. In the 1980s, ICT and OT operated in different environments and on different platforms. Specifically, OT systems were based on proprietary platforms – it was not until the 1990s that OT was networked to allow centralised operation. Starting in the early 2000s, however, OT systems began to connect to ICT systems using standardised channels to reduce costs and increase compatibility[16].With this convergence, what was relatively standalone secure and isolated environment is now connected and accessible via the Internet or cloud, and the vulnerabilities in ICT networks can be used to direct attacks on OT networks[17]. Within road transportation sector, the integration of legacy system and ITS have brought additional layers of complexity to the overall system infrastructure - the widening attack surface and increasing cybersecurity vulnerabilities as a result.

Cybersecurity Challenges Common to CI Sectors

OT networks and systems are commonly used in CI sectors, such as energy, utilities, water, and transportation. Theses systems are often highly engineered and use proprietary protocols that are specific to project requirements[18]. Many control systems follow standards, protocols and software designed and at

[12] Recent trends in intelligent transportation systems: a review: https://www.researchgate.net/publication/279277478_Recent_trends_in_intelligent_transportation_systems_a_review

[13] University of Michigan Transportation Research Institute: http://www.umtri.umich.edu/our-focus/advanced-traffic-management-systems

[14] Recent trends in intelligent transportation systems: a review: https://www.researchgate.net/publication/279277478_Recent_trends_in_intelligent_transportation_systems_a_review

[15] Recent trends in intelligent transportation systems: a review: https://www.researchgate.net/publication/279277478_Recent_trends_in_intelligent_transportation_systems_a_review

[16] Cyber savvy: Securing operational technology assets. PwC (2015)

[17] The convergence of IT and OT in critical infrastructure https://ro.ecu.edu.au/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1217&context=ism

[18] ibid.

a time when there were limited interconnections between devices and networks[19]. As a result of ICT and OT convergence, systems that were previously closed are now layered, linked and exposed to all the risks that have existed in the ICT space for years[20]. For instance, in energy sector, critical control mechanisms and information such as pressures, temperatures, proximity, levels and sensor signals are now significantly vulnerable to cyber-attacks due to the increasing system connectivity.

The following represents some of the most common cybersecurity vulnerabilities within CI sectors:

- **Wireless communication:** Wireless technologies are based on a common physical resource, Radio Frequency (RF) Spectrum.[21] As RF Spectrum can be accessed by anyone, cyber vulnerabilities have emerged.

- **Integration of physical and virtual layers:** As OT is networked, it allows remote system monitoring, control, and data transmission. This results in increasing connectivity and multi-directional data flows via a large number of system access points[22].

- **Automation and new potential vulnerabilities:** Increased automation and connectivity improves safety by removing the possibility of human error. However, it also introduces new vulnerabilities due to the increased number of system access points and, therefore, the widening attack surface[23].

- **Personal information and privacy:** Because CI sectors like Banking, Health, ICT, and Road Transportation constantly interact with the public, they collect personal data of users. Ill-equipped cybersecurity infrastructure can result in data privacy vulnerabilities.

- **Embedded software (Firmware):** As more of the OT systems within CI sectors contain embedded software, the complexity and risk of managing firmware updates can become an issue into its own. New firmware updates can introduce new cybersecurity risks, yet delaying firmware updates can leave identified and mitigated vulnerabilities exposed. Such vulnerability also extends to digital maintenance tools that are used to calibrate and test OT systems[24].

Unique Cybersecurity Challenges within Road Infrastructure

Road transportation networks face unique cybersecurity challenges partially due to broad networks, and integration of legacy system and ITS. These challenges primarily fall under the following categories:

- **Unauthorized access to physical infrastructure:** With Canada's extensive road network, it is challenging to monitor and secure the entire physical infrastructure facilities, such as cameras, traffic signal control cabinets and variable-message signs.

- **Multiple interdependent systems:** Road transportation networks are comprised of interconnected networks like sensors, cameras, financial systems, and emergency systems. However, many of these systems operate interdependently, meaning that a vulnerability with one system can impact several others[25].

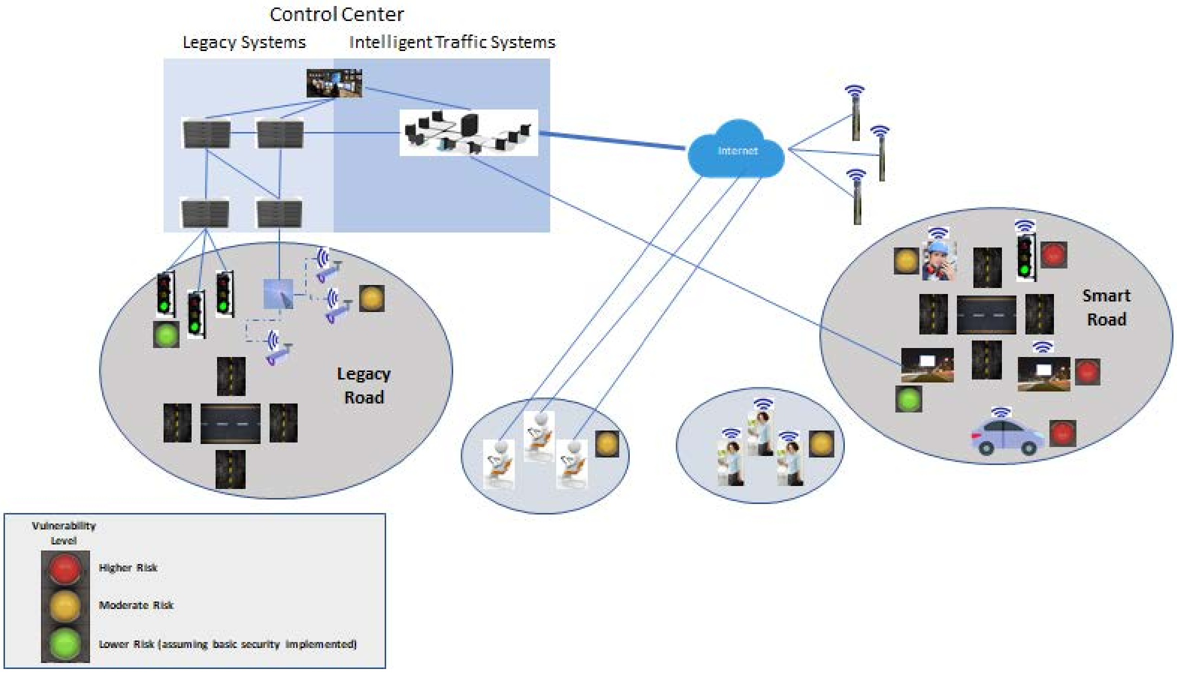
- **Integration of ITS into legacy systems:** The integration of ITS into legacy systems brings complexity to the overall system infrastructure. In turn, this system complexity creates issues with system recovery and redundancy, making it challenging to create automatic protections from new threats[26].

[19] ibid.
[20] ibid.
[21] Wireless Communications Cyber Security https://www.psc-europe.eu/images/DLCyberWirelessPaper.pdf
[22] US Department of Homeland Security, "The Future of Smart Cities".
[23] Cyber Security and Resilience of Intelligent Public Transport.https://www.enisa.europa.eu/publications/good-practices-recommendations
[24] AINonline: Companies Look to Blockchain To Secure Supply Chains, https://www.ainonline.com/aviation-news/aerospace/2018-07-12/companies-look-blockchain-secure-supply-chains
[25] ibid.
[26] ibid.

- **Embedded software (Firmware) update challenges:** As ITS evolves, so does the need to apply firmware updates or patching to fix known system risks or add new features. However, it is challenging to conduct thorough validation testing among the entire road transportation infrastructure, before implementing firmware updates. Without adequate validation testing, firmware updates are likely to introduce new cybersecurity vulnerabilities.

Graphic 1.2 below showcases the cybersecurity vulnerabilities that can arise within road infrastructure, as a result of the integration of ITS and legacy systems.

Graphic 1.2



Opportunities and Challenges in the CV and AV Era

The emergence of automated and connected vehicles - although still yet to be fully integrated within the mainstream mode of vehicular transport - has ushered in a new era of technological innovation that is continuously evolving and developing. AVs, also known as automated or self-driving vehicles, are those which rely on sensors (such as radar and cameras) and computer analytics to sense their environments and navigate without human input.[27] Today, there are vehicles that are already being deployed with varying degrees of automated functionality, such as self-parking, and auto-collision avoidance. The level of automation varies between level zero (no automation), up to level 5 (full automation) where the driving functions are fully controlled by an automated driving system.

CVs use wireless technology to facilitate vehicle-to-vehicle (V2V) and vehicle-to-infrastructure communications (V2I).[28] These vehicles are embedded with a number of different communication devices that enable in-car connectivity.[29]A significant feature of connected vehicles is that the underlying technology is able to facilitate the exchange of information in real time, allowing motorists to make safer and more informed travel decisions. These vehicles have the capacity to collect and transmit large volumes of data related to vehicle speed, location, and overall road condition information – data that can be accessed and leveraged by road authorities to more efficiently manage traffic flow. Graphic 1.1 below illustrates the

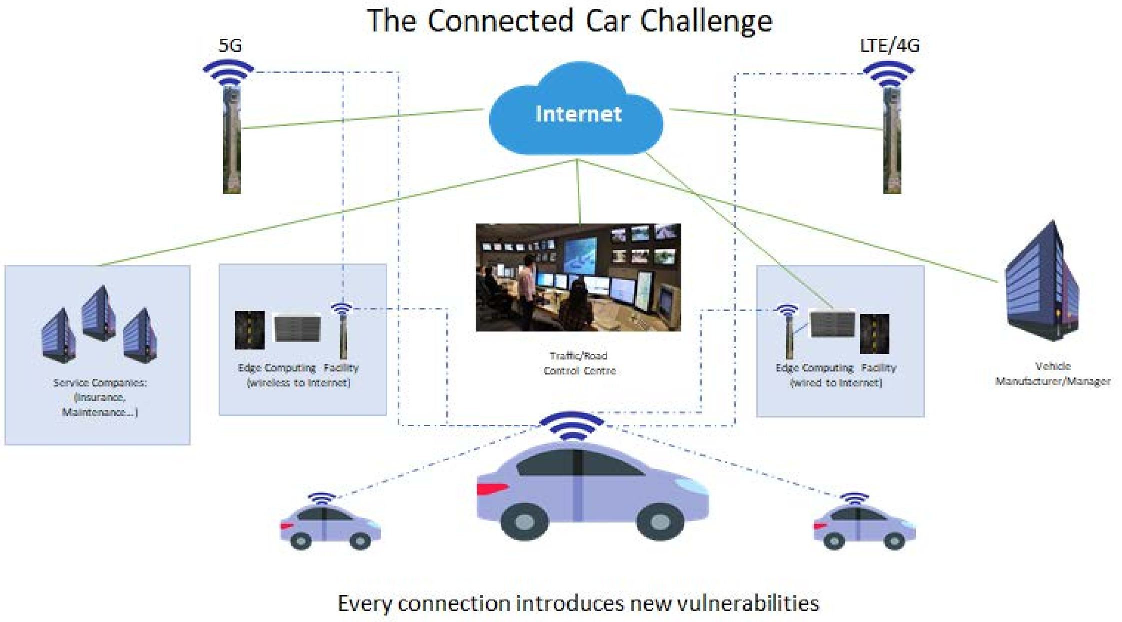
[27] Automated and Connected Vehicles: Status of the Technology and Key Policy Issues for Canadian Governments: https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/201698E

[28] Automated and Connected Vehicles: Status of the Technology and Key Policy Issues for Canadian Governments: https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/201698E

[29] The Institute of Electrical and Electronics Engineers: http://sites.ieee.org/connected-vehicles/ieee-connected-vechicles/connected-vehicles/

relationship between the connected car and its external environment.

Graphic 1.1


The Connected Car Challenge
5G
LTE/4G
Internet
Service Companies: (Insurance, Maintenance...)
Edge Computing Facility (wireless to Internet)
Traffic/Road Control Centre
Edge Computing Facility (wired to Internet)
Vehicle Manufacturer/Manager
Every connection introduces new vulnerabilities

From a cybersecurity perspective, automated and connected vehicles face a number of unique security challenges that create both societal and business risks. The underlying technologies that enable automated functionalities opens up the possibility for remote access via cyber intrusions that can exploit system vulnerabilities as the level of connectivity increases. As mentioned earlier, a standard feature of these vehicles is their capacity to store and exchange large volumes of information. This may include data on vehicle travel patterns, location tracking, and even passenger biometric data. Other cyber-related threats may also include forged vehicle communications, sensor jamming and blinding that may limit the vehicle's awareness of its surroundings.[30] Although these threats may appear to be somewhat benign on the surface, they do have the potential to cause personal injury and significant damage to road transportation networks by way disrupting traffic flow and more importantly undermining the safety of the transport system as whole. With public safety being an important component of the mandate that has been given to road authorities; the establishment of specific standards and regulations that address safety issues relating to the deployment of automated and connected vehicles on public roads will therefore be a policy area for which road authorities will have increasing responsibility.

Additionally, road authorities will need to take a proactive approach, by making investments in operational devices and hardware systems. This can allow for the proper integration of new technologies within the network of connected infrastructure. Additionally, with real time data sharing being an important component of these innovative technologies, road authorities will also need to develop a comprehensive policy framework that sets out guidelines for access to and use of the data that is generated by these vehicles so as to protect the privacy rights of individuals.

1.3 Increasing Cybersecurity Attack Targeting Transportation Infrastructure

The Internet of Things, digitalization, smart cities, and the systems and technologies behind these developments have brought forward positive social outcomes and economic growth by increasing productivity. However, cyber-attacks towards critical infrastructure are increasing at a rapid pace, not just in Canada but around the world. At the same time, the nature of cyber-attacks has become more

[30] Protecting autonomous vehicles from cyber attacks: https://www.automotivetestingtechnologyinternational.com/features/vehicle-manufacturers-can-protect-autonomous-vehicles-potential-attacks.html

sophisticated, sometimes causing immeasurable damage. One of the more high-profile cyber-attacks occurred in 2017 when the Danish transport and logistics conglomerate Maersk was one of several companies that fell victim to a ransomware attack. This attack resulted in IT systems and operational controls beings compromised. It was reported that the company endured severe disruptions and was even forced to halt its operations as the ransomware spread throughout its core IT systems. Maersk, at the time, estimated that this cyber-attack would cost the company up to $300 million in lost revenues.[31]

Reports have also surfaced of several seemingly benign attacks on transport infrastructure in the US. In June 2014, at least three highway signs in North Carolina had been compromised, resulting in the electronic message that is usually displayed being changed by the perpetrator. Other incidents of a similar nature occurred in two other states around that time period.[32] There has also been an increase in incidents of cyber-attacks that appear to be benign in nature, but have exposed the underlying vulnerability of our critical infrastructure systems. An example of such an incident occurred in December 2015 when BC's Transit computer systems were hacked, resulting in the transit operator having to shutdown its networks. [33]

The trend of these public incidents is that many sectors are now becoming more aware of their own cyber vulnerabilities. As a by-product of this, many sectors and businesses are scrambling to safeguard themselves against potential attacks. As road transportation is the most commonly-used transportation system in Canada, it is of considerable importance that Canadian road authorities secure a robust grounding of cybersecurity talent in order to ensure the physical and cybersecurity of the Canadian road transportation system.

Part 2: Cybersecurity Challenges and Talent Development Needs for Canadian Road Authorities - Case Study Based on Key Informational Interviews[34] (KIIs)

2.1 How are Canadian road authorities acquiring or developing the necessary talent?

General IT Treatment vs. Cybersecurity Practice Applicable to ITS

The results of our KII suggest there are significant challenges to applying cybersecurity practices in road transportation. The Canadian road authorities interviewed in this study have relied on their internal IT departments to provide services and support like monitoring, investigating and remediating cyber incidents. The transportation departments interviewed stated that they would often treat cyber incidents the same way they would treat any IT or OT problem – with a common response being to constantly update and repair the road transportation system, regardless of the root causes of the incidents. When asked why this was the case, informants suggested that this was because when a problem occurred, it was difficult for road authorities to identify if it was caused by cybersecurity breaches or by common OT system issues like malfunctions of sensors and systems. This suggests the absence of an OT cybersecurity framework among the road authorities interviewed.

[31] NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#5fb286b64f9a
[32] They Hack Because They Can https://krebsonsecurity.com/2014/06/they-hack-because-they-can/
[33] BC Transit increases cybersecurity after threat http://www.thetransitwire.com/2016/02/02/bc-transit-increases-cybersecurity-after-threat/
[34] For KII methodology, please see Appendix B

General Cybersecurity Training vs. Industry-Specific Cybersecurity Training Applicable for Road Transportation Sector

Online training and conferencing were the most common ways for Canadian road authorities consulted to get updates regarding new technologies and network development in the field. Canadian road authorities interviewed in this study stated that they have relied on agencies like the U.S. National Institute of Standards and Technology (NIST) and multinational technology companies to provide industry feedback and advice on functionality and security of road transportation networks. There was also a consensus among interviewees that there is no industry-specific cybersecurity training or programs available for them, but that the need for such programs exist.

2.2 The Three Pillars of Cybersecurity Talent Development for Canadian Road Authorities

There are a number of cybersecurity talent and skill needs that Canadian road authorities possess when it comes to protecting their OT assets and IT infrastructure. Based on consultations with industry experts, this study offers a three- pillar approach related to cybersecurity talent development for Canadian road authorities:

Pillar 1: Cybersecurity Awareness Training and Education for Non-Cybersecurity Specific Talents

Canadian road authorities must source and develop cybersecurity professionals that can work in collaboration with traditional OT engineers and IT professionals. Transportation-related cybersecurity needs are unique and require the following specific sets of expertise:

- Deep cybersecurity knowledge:
    - Network topology and security
    - Traditional cryptography and quantum-safe cryptography
    - Attack surface evaluation
    - Threat assessment
    - Intrusion detection
    - Operating system and programming language weaknesses
- Expertise related to transportation and road security:
    - Security of field technology
    - Wireless protocols
    - Advanced traffic/transportation systems
- The ability to adapt to the rapid rate of evolution of cybersecurity threats and technologies:
    - Staying current with cybersecurity resources like the Canadian Centre for Cyber Security[35] and U.K.'s National Cyber Security Centre[36]
    - Stay up-to-date with new developments in cybersecurity hardware, software, platforms and services

Moreover, it is also clear that non-cybersecurity specific talent, such as road authority managers, OT and IT professionals, will also need basic cybersecurity awareness training and education. This is required in order to understand the importance of cybersecurity in an OT environment, help identify threats alongside

[35] Canadian Centre for Cyber Security: Alerts and Advisories, https://www.cyber.gc.ca/en/alerts-advisories

[36] National Cyber Security Centre: Alerts and Advisories, https://www.ncsc.gov.uk/index/alerts-and-advisories

cybersecurity professionals, and include cybersecurity into operations and projects during the design process. Our consultations identified the following types of cybersecurity training and certifications existing road authority professionals should consider:

- The Canadian Centre for Cyber Security training, available through their Learning and Innovation Hub (LIH). The LIH is featured in providing adaptable learning pathways which have been developed to help security practitioners, supervisors and managers identify learning activities that will support cybersecurity knowledge and skill development. Additionally, LIH has broadened their mandate to include cybersecurity curriculum guidance to academia and industry with a focus on critical infrastructure [37].
- The (ISC)^2 Certified Information System Security Professional (CISSP). CISSP is designed for experienced security practitioners, manager and executives, with a focus to equip them with a wide array of security practices and principles.[38]

In the interviews, industry experts stressed that road authorities do not need their transportation engineers to be cybersecurity experts per se, but they do need to be aware of how cybersecurity fits into the bigger picture of transportation infrastructure.

One of the most important skills for cybersecurity professionals and road authority management identified throughout the interviews was risk management. There is no OT or OT-IT system that is 100% secure, making it important to apply a risk management methodology such as monitoring and reporting potential threats, to each instance[39]. One interviewee shared that road authorities needed to integrate risk management methodologies into their cybersecurity strategies. Doing so will tie together the applications of cybersecurity practices for the average person without a cybersecurity background.

Cybersecurity roles are, in general, informally defined by the broader cybersecurity industry. This means that there is no “one” core definition of cybersecurity or a cybersecurity professional. However, a useful overview of cybersecurity roles and their requisite skills and certifications can be found on the U.S. Cybersecurity Career Pathway, created by for the National Initiative for Cybersecurity Education (NICE), a program of the NIST in the U.S. Department of Commerce[40].

Pillar 2: Establish Cybersecurity Framework and Protocol

Before implementing a cybersecurity policy and infrastructure, it is important to establish a baseline assessment of the existing OT systems and environment. One of the most important components to assess is the OT-IT demilitarized zone (DMZ)/ boundary since IT approaches to cybersecurity are different from OT considerations. For instance, the priority in the IT space is to protect data, but in the OT space, the priority is to protect the asset base and its associated production[41].

[37] Canadian Center for Cyber Security: Learning and Innovation Hub https://www.cyber.gc.ca/en/learning-and-innovation-hub

[38] (ISC)^2: CISSP - Certified Information Systems Security Professional https://www.isc2.org/Certifications/CISSP

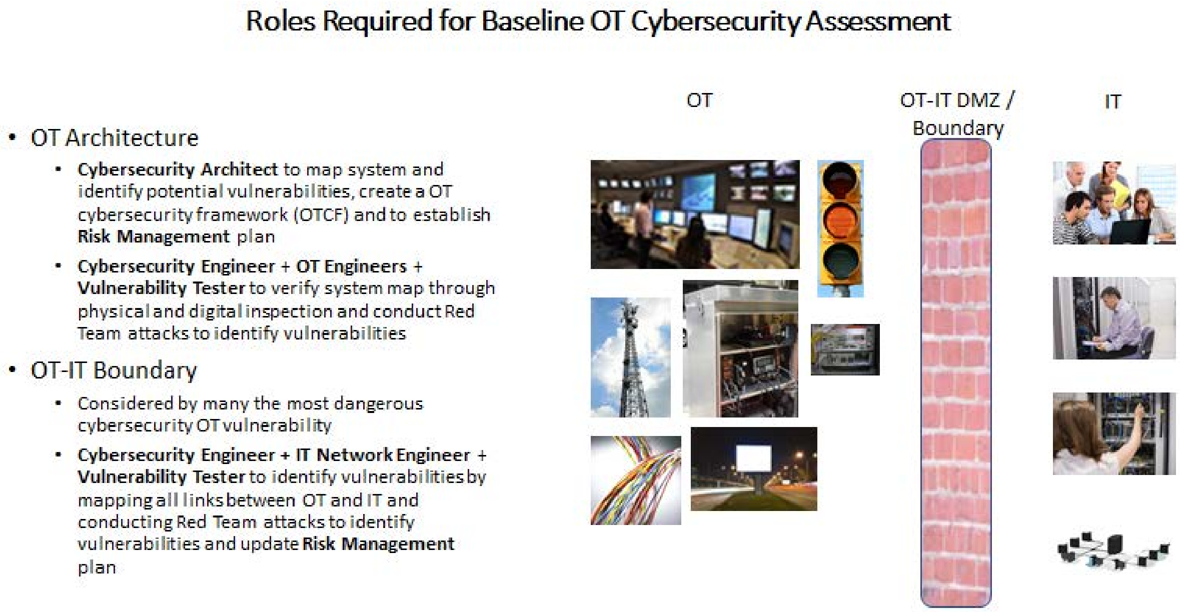
[39] For more details about establishing a Cybersecurity Risk Management Plan, please refer Part 5 of the report

[40] CyberSeek: Cybersecurity Career Pathway https://www.cyberseek.org/pathway.html

[41] The Convergence of IT and OT in Critical Infrastructure https://ro.ecu.edu.au/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1217&context=ism

Graphic 2.1 below showcases the roles (and job descriptions) most in-demand for a baseline OT cybersecurity assessment.

Graphic 2.1



Roles Required for Baseline OT Cybersecurity Assessment

- OT Architecture
  - **Cybersecurity Architect** to map system and identify potential vulnerabilities, create a OT cybersecurity framework (OTCF) and to establish **Risk Management** plan
  - **Cybersecurity Engineer** + **OT Engineers** + **Vulnerability Tester** to verify system map through physical and digital inspection and conduct Red Team attacks to identify vulnerabilities
- OT-IT Boundary
  - Considered by many the most dangerous cybersecurity OT vulnerability
  - **Cybersecurity Engineer** + **IT Network Engineer** + **Vulnerability Tester** to identify vulnerabilities by mapping all links between OT and IT and conducting Red Team attacks to identify vulnerabilities and update **Risk Management** plan

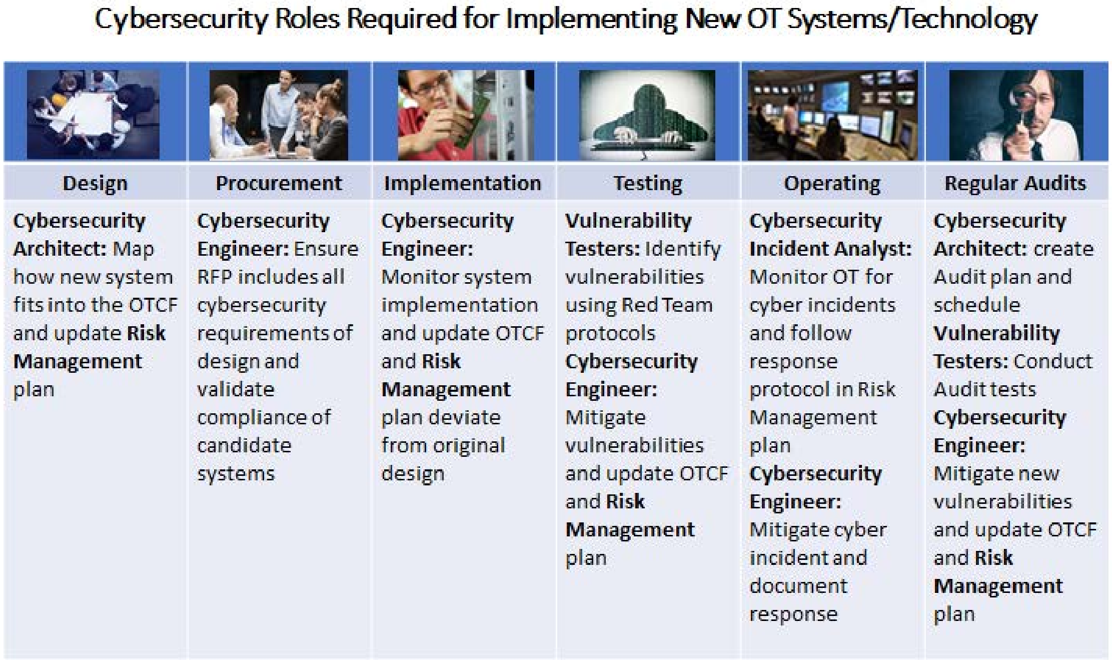
Ideally, the deliverables from such an exercise would be: the creation of an OT Cybersecurity Framework (OTCF) that maps all aspects of cybersecurity in the OT assets and infrastructure; and, a Cybersecurity Risk Management Plan that details all vulnerabilities, ranked by threat potential. These two deliverables set the foundation for the creation of all cybersecurity policies, processes and procedures.

Cybersecurity Protocol for Legacy System and ITS integration

It is important to have a protocol for dealing with potential cybersecurity implications that come with deploying new technologies and services into the OT infrastructure. It is important for the cybersecurity professionals to work closely with the OT operations and field engineers to facilitate knowledge sharing and transfer.

Graphic 2.2 below highlights the most important cybersecurity roles required when implementing new OT systems and technologies.

Graphic 2.2



Cybersecurity Roles Required for Implementing New OT Systems/Technology

Design	Procurement	Implementation	Testing	Operating	Regular Audits
Cybersecurity Architect: Map how new system fits into the OTCF and update **Risk Management** plan	**Cybersecurity Engineer:** Ensure RFP includes all cybersecurity requirements of design and validate compliance of candidate systems	**Cybersecurity Engineer:** Monitor system implementation and update OTCF and **Risk Management** plan deviate from original design	**Vulnerability Testers:** Identify vulnerabilities using Red Team protocols **Cybersecurity Engineer:** Mitigate vulnerabilities and update OTCF and **Risk Management** plan	**Cybersecurity Incident Analyst:** Monitor OT for cyber incidents and follow response protocol in Risk Management plan **Cybersecurity Engineer:** Mitigate cyber incident and document response	**Cybersecurity Architect:** create Audit plan and schedule **Vulnerability Testers:** Conduct Audit tests **Cybersecurity Engineer:** Mitigate new vulnerabilities and update OTCF and **Risk Management** plan

Top In-demand Cybersecurity Roles to Canadian Road Authorities

The most applicable cybersecurity roles for Canadian road authorities were identified via an analysis of key informant interviews and secondary research. This was complemented with results from cybersecurity job postings from other jurisdictions, in relation to road authorities. These are:

1. Cybersecurity Architect

    - Responsible for architecting and documenting the OTCF. The OTCF is the OT system map of the OT environment from a cybersecurity perspective.
    - Responsible for creating a cybersecurity Risk Management plan
    - Possesses deep knowledge of standards like ISO 27000[42], the NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1[43], Canada's CSA-led Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program CAN/CSA-IEC 62443-2-1[44], and the in-development standards like the Institute of Transportation Engineers (ITE)-led Roadway Transportation Systems Cybersecurity Framework[45].
    - Possesses industry certifications like the Global Information Assurance Certification (GIAC)

[42] International Organization for Standardization: ISO/IEC 27000 family - Information security management systems, https://www.iso.org/isoiec-27001-information-security.html

[43] NIST: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

[44] Standards Council of Canada: CAN/CSA-IEC 62443-2-1:17, https://www.scc.ca/en/standardsdb/standards/29106

[45] ITE: Transportation System Management and Operations, https://www.ite.org/technical-resources/topics/transportation-system-management-and-operations/

for Critical Infrastructure Protection (GCIP)[46], the ISACA Certified Information Systems Auditor (CISA)[47], the ISACA Certified Information Security Manager (CISM)[48], and the Security+ certifications[49].

- Possesses expert knowledge on network security, cryptography, systems architecture, and information security.
- Should have familiarity of transportation OTs.

2. **Cybersecurity Engineer**

- Responsible for mitigating cybersecurity vulnerabilities and managing cybersecurity architecture.
- Possesses experience with and follow standards like ISO 27000, the NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, Canada's CSA-led Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program CAN/CSA-IEC 62443-2-1, and the in-development standards like the Institute of Transportation Engineers (ITE)-led Roadway Transportation Systems Cybersecurity Framework[50].
- Has industry certifications like the Global Information Assurance Certification (GIAC) for Critical Infrastructure Protection (GCIP)[51], the (ISC)^2 Certified Information System Security Professional (CISSP)[52] and the Security+ certifications[53].
- Should have experience managing risk management system.
- Possesses hands-on experience with network (both wired and wireless) and information security, programming and scripting skills, solid knowledge of access control, authentication, and cryptography.
- Should have familiarity of OT technologies and work closely with Transportation Engineers to better understand control centre and field OT technologies.

3. **Vulnerability Tester**

- Responsible for conducting and documenting vulnerability tests
- Should have industry certifications like the Certified Ethical Hacker[54], the Licensed Penetration Tester[55], GIAC Web Application Penetration Tester (GWAPT)[56], and the PenTest+[57].
- Has experience with vulnerability assessment, penetration testing, networking protocols, data analytics, data management, data security, coding and scripting, access control, authentication protocols, cryptography, and Intrusion Detection and Prevention Systems.
- Needs to work closely with Transportation Engineers to better understand control centre and

[46] GIAC: GIAC Critical Infrastructure Protection, https://www.giac.org/certification/critical-infrastructure-protection-gcip

[47] ISACA: Certified Information Systems Auditor, https://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx

[48] ISACA: Certified Information Security Manager, http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx

[49] CompTIA: CompTIA Security+, https://certification.comptia.org/certifications/security

[50] Roadway Transportation Systems Cybersecurity https://www.ite.org/technical-resources/topics/transportation-system-management-and-operations/

[51] GIAC: GIAC Critical Infrastructure Protection, https://www.giac.org/certification/critical-infrastructure-protection-gcip

[52] (ISC)^2: Certified Information Systems Security Professional, https://www.isc2.org/Certifications/CISSP

[53] CompTIA: CompTIA Security+, https://certification.comptia.org/certifications/security

[54] EC-Council: Certified Ethical Hacker, https://www.eccouncil.org/programs/certified-ethical-hacker-ceh-practical/

[55] Ibid.

[56] GIAC: GIAC Web Application Penetration Tester, https://www.giac.org/certification/web-application-penetration-tester-gwapt

[57] CompTIA: CompTIA PenTest+, https://certification.comptia.org/certifications/pentest

field OT technologies.

4. **Cybersecurity Incident Analyst**

    - Responsible for monitoring the cybersecurity health of the OT operations and field systems.
    - Possesses the ability to respond to cybersecurity incidents, including logging and initiating the incident response protocol from the Risk Management plan.
    - Should have industry certification like GIAC's Certified Incident Handler (GCIH)[58], the EC-Council Certified Incident Handler (ECIH)[59] and the National Initiative for Cybersecurity Careers and Studies (NICCS) Certified Cyber Threat Analyst[60].
    - Has experience with Intrusion Detection and Prevention Systems and cybersecurity monitoring solutions.

Pillar 3: Develop a Cybersecurity Resource Pool - External Experts

One key consideration in the development of cybersecurity talent for road infrastructure needs is that the cybersecurity resources do not have to be permanent road authority employees. Instead, they can be contractors who are sourced for specific projects or needs. According to one interviewee, some of the larger U.S. state Departments of Transportation (DOTs) outsource a portion of their cybersecurity roles. The interviewee stressed that it is important to encourage the development of a cybersecurity consultant ecosystem – not necessarily full-time employees. This network of consultants was seen as helping to augment and shape the road authorities' (and the government in general) cybersecurity talent pool.

The CV Era and More Cybersecurity Challenges to Come

Lastly, the realization of a fully-operational connected vehicle (CV) system will undoubtedly introduce an exponential increase in OT cybersecurity vulnerability. Under this reality, road authorities may have to support multiple and very different wireless protocols including 4G/LTE, 5G, and DSRC. This is especially the case in Canada where 5G infrastructure and deployment is lagging behind many industrialized countries[61]. 5G will possess some cybersecurity improvements over previous generations of telecommunication technologies, yet the introduction of software-based technologies replacing physical systems (i.e. Software Defined Networks) will create new threats and exploits for cyber attackers. Before CV infrastructure is fully deployed, road authorities should acquire cybersecurity resources, either full-time or contract, that understand all wireless protocols. These protocols include the networking capabilities and architectures of the vehicles themselves, the threats introduced by other applications that may share the wireless infrastructure with road authorities, and knowledge of how these factors integrate with the OT systems.

2.3 Existing Cybersecurity Skill and Knowledge Development Programs

In Canada, similar to many jurisdictions, it is widely acknowledged that there is a critical shortage of cybersecurity professionals across sectors. Broadly speaking, the current demand for these individuals in

[58] GIAC: GIAC Certified Incident Handler, https://www.giac.org/certification/certified-incident-handler-gcih

[59] EC-Council: EC-Council Certified Incident Handler, https://www.eccouncil.org/programs/ec-council-certified-incident-handler-ecih/

[60] NICCS: Certified Cyber Threat Analyst, https://niccs.us-cert.gov/training/search/mcafee-institute/certified-cyber-threat-analyst-ccta#

[61] ICTC-CTIC: 5G: Jumpstarting our Digital Future, https://www.ictc-ctic.ca/wp-content/uploads/2018/12/ICTC_5G-Jumpstart-our-Digital-Future_EN-12.4.18.pdf

both the private and public sectors far outweighs the supply. Recent studies have indicated that this trend is expected to continue into the foreseeable future, with the labour market imbalance beginning to take shape in this particular segment of the Canadian workforce.[62]

While there have been a number of initiatives are beginning to take shape to correct this imbalance, there is still work that needs to be done to ensure a stable supply of talent to meet demand. At the same time, these developments have brought sharply into focus of the need to identify, develop and nurture the next generation of cybersecurity professionals. This is a philosophy that is already being embraced by a number of Canadian academic institutions, who through the development and integration of cybersecurity related courses and programs, have been responding to this challenge.

Some of the academic institutions taking this approach include the University of New Brunswick, responsible for the Canadian Institute for Cybersecurity (CIC). This is a multidisciplinary training, research and development centre that brings together researchers and practitioners from across the academic spectrum, as well as industry to conduct ground-breaking research and skills training in the area of cybersecurity.[63] There are also a number of other prominent institutions such as the University of Toronto[64], McGill University[65], and the University of British Columbia[66] that currently have courses or programs geared towards developing highly-skilled cybersecurity professionals. For instance, the University of Toronto offers a certificate program in cybersecurity management, teaching individuals how to develop and run effective security programs that align with different business processes and cycles. This program also allows individuals to upgrade their knowledge in risk assessment and response, security program design, incident and risk management, along with other areas related to security compliance and governance.

McGill University offers a course in computer network and Internet security that deals with the principles surrounding the design and performance of computer networks. Other areas of focus in this particular course include the theory and technology behind network security models, cryptography protocols, security counter-measure strategies and tools, as well as access control and platform-specific security issues. In fact, a few years ago, SERENE-RISC, a cybersecurity umbrella organization identified approximately 450 cybersecurity related courses that were being taught in over 60 Canadian universities.[67] A number of colleges have also incorporated cybersecurity into their computer science curriculums. These include Nova Scotia Community College, Centennial, Fanshawe, Seneca, Conestoga, Cégep de Sainte-Foy, and the Collège Communautaire du Nouveau-Brunswick. Although the courses offered by these institutions aren't necessarily designed to address the cyber-related concerns that are specific to the transport sector, they do provide a solid grounding in the core concepts as well a as a comprehensive overview of the issues surrounding cybersecurity as whole. Other courses are available outside of Canada that are tailor-made to address cybersecurity in the context of the transportation sector. One such course is currently being offered by the Consortium for Innovative Transportation Education (CITE) in collaboration with the U.S. Department of Transportation. This particular course, entitled Transportation Cyber Security, is designed for professionals working with surface transportation systems, and is geared towards improving the understanding of the complex and rapidly changing technologies associated with the broad discipline of cybersecurity.[68]

SERENE-RISC is also playing its part in the area of skills development. The organization, through its integrated network of academic and industry experts, offers professional development activities in the area of cybersecurity to graduate students and early career government and private sector employees. These activities are aimed at providing opportunities for individuals to stay abreast with the latest developments in the field.[69]

[62] The changing faces of cybersecurity – Closing the cyber risk gap: https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF

[63] University of New Brunswick, Canadian Institute for Cyber Security: https://www.unb.ca/cic/about/index.html

[64] University of Toronto: https://learn.utoronto.ca/programs-courses/certificates/cyber-security-management

[65] McGill University: https://www.mcgill.ca/study/2018-2019/courses/ccs2-510

[66] University of British Columbia: https://www.ece.ubc.ca/course/cpen-442

[67] The changing faces of cybersecurity - Closing the cyber risk gap: https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF

[68] Consortium for Innovative Transportation: http://www.citeconsortium.org/course/cyber-security/

[69] SERENE-RISC: https://www.serene-risc.ca/en/about-us/six-key-activities

Part 3: Examining Cybersecurity Talent and Skill Gaps among Canadian Road Authorities

The goal of this section is to determine the cybersecurity skills currently present in the transportation sector. This data was collected by scanning profiles of individuals under transportation cybersecurity occupational categories, on professional job sites. A first attempt to gather information from Canada and Australia (an international case study for this report) resulted in only a few people in the transportation sector claiming to have cybersecurity as a skillset and provided little informational value. The lack of Canadian and Australian cybersecurity resources in the Transportation sector found on job sites may be due to a few factors, including but not limited to the following:

1. The Canadian and Australian transportation sectors are only beginning to implement cybersecurity strategically, and as a result, cybersecurity-specific roles are falling to existing IT resources in the interim.
2. Canadian and Australian transportation workers are not featuring, or have not updated their cybersecurity skills on their professional profile

In order to obtain a useful sample of profiles from a jurisdiction with similar transportation sector requirements to Canada, the U.S. transportation sector was scanned.

Methodology:

This study found 512 self-identified U.S. transportation workers with some form of cybersecurity experience in their online profile on a popular job site. An approximately 20% sample (due to this being an extensively manual process) was randomly selected from the 512 workers, resulting in a sample of 98 workers. All pre-categorized skills were collected for each of the sampled workers and tabulated to determine the skills most represented in the population. The data was then filtered to remove all non-cybersecurity skills, and the portion (%) of workers possessing each cybersecurity skill was calculated. Table 1 below showcases the cybersecurity-related skills found among a selection of online job profiles of US transportation sector workers.

Table 1. Cybersecurity Skills Listed on Job Profiles of Self-Identified U.S. Transportation Sector Workers

Skills	Skill Descriptions	% Workers with Such Skills
Network Security	Network Security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment.[70]	24%
Information Security	Information security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.[71]	22%
Integration	Integration of technologies, systems and services.	21%

[70] CSO: Network Security Resources, https://www.sans.org/network-securit

[71] Legal Information Institute: Legal Information Institute, https://www.law.cornell.edu/uscode/text/44/3542

Information Technology Infrastructure Library (ITIL)	ITIL is a widely accepted approach to IT Service Management (ITSM) provides guidance to organizations and individuals on how to use IT as a tool to facilitate business change, transformation and growth.[72]	10%
Risk Assessment	Analyzing the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.[73]	10%
Risk Management	Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impacts. With this information, organizations can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk tolerance.[74]	10%
Systems Engineering	Systems Engineering is an interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, then proceeding with design synthesis and system validation.[75]	7%
CISSP	Certified Information Systems Security Professional (offered by the International Information System Security Certification Consortium, or (ISC)^{2}).	7%
Penetration Testing	Penetration testing (a.k.a. pen testing or ethical hacking) is a practice undertaken by professional hackers to find the vulnerabilities in your systems - before the attackers do.[76]	5%
Network Engineering	The design and management of networks.	5%
Vulnerability Assessment	A vulnerability assessment is the process of identifying and analyzing those security vulnerabilities that might exist in the enterprise. Vulnerability assessments are typically conducted through network-based or host-based methods, using automated scanning tools to conduct discovery, testing, analysis and reporting of systems and vulnerabilities.[77]	5%

[72] Axelos: What is ITIL® Best Practice, https://www.axelos.com/best-practice-solutions/itil/what-is-itil

[73] NIST Cybersecurity Framework: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[74] NIST Cybersecurity Framework: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[75] The Internet Society: What is Encryption, https://www.Internetsociety.org/issues/encryption/

[76] TechTarget: security audit, https://searchcio.techtarget.com/definition/security-audit

[77] TechTarget: sensor, https://whatis.techtarget.com/definition/sensor

System Architecture	System architecture is the conceptual representation of a system's components and how they interact both between each other and externally.	5%
Certified Ethical Hacker (CEH)	CEH is a qualification obtained by demonstrating knowledge of assessing the security of computer systems by looking for weaknesses and vulnerabilities in target systems, using the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system. (CEH is offered by EC-Council[78])	4%
Intrusion Detection	Intrusion detection helps a network administrator establish not only where the attempted breach originates but also the tool or tools used.[79]	4%
Incident Response	Experience dealing with cybersecurity incidents.	3%
Physical Security	Securing physical OT assets like Operations Control Centre, Control Cabinets and Dynamic Digital Messaging signs.	3%
Security+	An IT security certification offered by CompTIA.	3%
Encryption	Encryption is the process of scrambling or enciphering data so it can be read only by someone with the means to return it to its original state.[80]	3%
Security Audits	A security audit is a systematic evaluation of the security of a company's information system by measuring how well it conforms to a set of established criteria. A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes, and user practices.[81]	3%
IT Risk Management	Risk management (described above) from the IT perspective.	2%
Sensors	A sensor is a device that detects and responds to some type of input from the physical environment. The specific input could be light, heat, motion, moisture, pressure, or any one of a great number of other environmental phenomena. The output is generally a signal that is converted to human-readable display at the sensor location or transmitted electronically over a network for reading or further processing.[82]	2%

The above highlights the skills that self-identified cybersecurity workers within the Transportation sector currently possess. Compared to the cybersecurity skills profiled in Section 2, the above tables show that the

[78] Certified Ethical Hacker Certification https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
[79] NAIT: Intrusion Detection/Prevention, http://www.nait.ca/course_CCTM490.htm
[80] The Internet Society: What is Encryption, https://www.Internetsociety.org/issues/encryption/
[81] TechTarget: security audit, https://searchcio.techtarget.com/definition/security-audit
[82] TechTarget: sensor, https://whatis.techtarget.com/definition/sensor

transportation sector does not appear to have adequate cybersecurity skills in-house. Traditional IT security skills like Network Security and Information Security were best represented, yet desirable cybersecurity skills like Risk Assessment, Vulnerability Assessment, Penetration Testing and Intrusion Detection were not as well represented nor were the cybersecurity certifications including CISSP, CEH and Security+.

A second data collection phase attempted to collect data from transportation sector cybersecurity job postings and transportation sector technical jobs. This collection identified the fact that very few transportation job postings even require cybersecurity skills – as in they are not mentioned in the job description[83]. This is consistent with feedback from our consultations, which identified that road authorities significantly trail other Critical Infrastructure (CI) sectors in technology (including cybersecurity) awareness and adoption.

Part 4: Case Studies: An International Perspective for Canada

4.1 How are other jurisdictions approaching the need for talent development in this area?

The UK Approach

The ever-evolving nature of cyber-attacks has highlighted the need to have the right mechanisms in place to safeguard against these threats. A 2017 cybersecurity report from the UK entitled Cyber Security Skills: Business Perspectives and Government's Next Steps, gathered information from over 1500 companies, and revealed that practically all of them were in some way exposed to cybersecurity risks.[84] Part of the reason for this stems from the proportion of companies that have websites or social media pages. While these platforms have been steadily increasing in popularity, the maintenance of these sites has remained minimal – something that leaves them open to vulnerabilities. Another reason was that many of these companies were utilizing cloud-based services that did not have the proper cybersecurity practices and protocols in place. It is within this context that the vast majority of these UK-based companies identified cybersecurity as a serious concern for their business' future.

Examining the talent component, having a senior individual in charge of cybersecurity matters (someone who can influence important decisions within the company), was one of the key needs identified. Moreover, while senior talent was sparse, a little under 40% of companies reported that they did have other staff tasked with handling cybersecurity issues. Another half of these companies noted outsourcing their cybersecurity functions.

On a broader and more policy-oriented level, the UK government as part of its National Cyber Security Strategy has outlined the need to support activities that are geared towards increasing cybersecurity skills across all levels of the education system. This is prioritized in order to develop the knowledge base and instill cybersecurity capacity as a core component under the wider national cyber strategy.[85] Through collaboration with different government agencies, private business, and educational institutions, the British government has funded various activities and created teaching materials that are geared towards promoting cybersecurity education and training in primary and secondary schools, with the goal of attracting individuals to the profession. Funding has also been allocated towards providing internship and apprenticeship opportunities for graduate and post-graduate students in order to enhance the skillsets of prospective new entrants into the profession. A key component of this initiative was centred on raising awareness about cybersecurity careers, while at the same time encouraging the participation of students in

[83] As an example, Appendix B include two job recent job posts from BC MOTI

[84] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

[85] Cyber Security Skills Business perspectives and Government's next steps: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-security-skills-business-perspectives-and-governments-next-steps.pdf

more technology-related areas of studies.

Developing a cutting-edge research capacity was also identified as a key component of the government's strategy for increasing cybersecurity skills and capability in the workforce. To this end, the government designated several universities as academic centres of excellence for cybersecurity research. Some of the more prominent universities that were designated as such includes Cambridge, Oxford, Edinburgh, and University of Birmingham. In general, the designation is awarded to institutions on the basis of having the capacity to enhance the quality and scale of academic cybersecurity research and postgraduate training that is being undertaken in the UK. Other minimum standards that these universities must meet includes having the academic staff with a proven track record of high-impact cybersecurity research in leading academic journals and conferences. [86] The government has also provided funding for doctoral training to develop advanced skills and capacity building initiatives at the high-end of the skills spectrum. Specifically, the Research Council UK has been funding Centres of Doctoral Training (CDTs) tasked with delivering multidisciplinary training to the next generation of cybersecurity experts. This aims to provide individuals with the knowledge and skillsets to both prevent and respond to incidents of cyber-related attacks. More importantly these institutions have been engaging the private sector on an ongoing basis in order to ensure that the training programs they deliver continue to take into account the complex and dynamic nature of the threats posed to cybersecurity.[87]

These and other initiatives are considered to be particularly important in relation to the UK government reaffirming its commitment towards enhancing the country's cybersecurity resilience across its critical national infrastructure (CNI) sectors. More so, there has been an increased focus on addressing this issue in light of a recent report that was published by the Joint Committee on National Security Strategy which highlighted as a cause for concern, the existing imbalance between the supply and demand for skilled cyber professionals and the impact that this was having across critical infrastructure sectors in the UK. The report mentioned that CNI operators and regulators highlighted the shortage in specialist skills and deep technical expertise as one of the biggest challenges they encounter in relation to addressing their cybersecurity concerns; with the acute scarcity of experts who understand the security implications of connecting legacy CNI control systems to the Internet being given as a prime example of the existing skills gap.[88]

The U.S. Approach

In the United States, cyber-related risks are becoming a growing concern among stakeholders in the transport sector and other critical infrastructure areas. Our consultations highlighted that there is an urgent need among road authorities to secure the necessary talent and skillsets to address these mounting concerns. However, there is a limited volume of cybersecurity talent employed by road authorities in the US, and many of these agencies outsource their cybersecurity functions to private companies. This is an approach which is mainly taken by road authorities in larger states. Smaller municipalities tend follow general IT best practices, rather than investing in cybersecurity talent. One reason for this "shortcut" was the misconception that being smaller, they are less exposed to cyber attacks, and are able to protect themselves with their own internal resources.

The US government has also embarked on a number of initiatives geared towards addressing the need for cybersecurity talent development. However, the approach that has been taken is more general, as opposed to focusing on the specific needs of particular sectors – in the US, cybersecurity issues tend to be treated as a matter of national security.[89] However, as part of its National Cyber Strategy, the US government highlighted a number of priority action plans that are geared towards developing a highly-skilled cybersecurity workforce. These include: investing in and enhancing programs that build the domestic talent pipeline from primary through to postsecondary education; and leveraging merit-based immigration reforms

[86] Engineering and Physical Sciences Research Council: https://epsrc.ukri.org/research/centres/acecybersecurity/

[87] Cyber Security Skills Business perspectives and Government's next steps: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-security-skills-business-perspectives-and-governments-next-steps.pdf

[88] Cyber Security Skills and the UK's Critical National Infrastructure. Second Report of Session 2017–19: https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/706/706.pdf

[89] National Cyber Strategy of the United States of America: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

in order to tap into the pool of foreign talent. Another important initiative policy focused on expanding reskilling and other educational opportunities for American workers. This is something that strives to afford people from a broad range of backgrounds the opportunity to re-train into cybersecurity careers.

Lastly, one priority area focused on enhancing the federal cybersecurity workforce by way of improving the recruitment and retention of highly qualified cybersecurity professionals. To this end, the government proposed to continue with the use of the National Initiative for Cybersecurity Education Framework to support policies that allow for a standardized approach to identifying, hiring, developing, and retaining cybersecurity talent; along with exploring various options for developing, managing, and deploying cybersecurity personnel across different federal departments and agencies. The government is also promoting improved compensation for federal workers with cybersecurity skills, along with unique training and operational opportunities to attract and retain critical cybersecurity talent.[90]

4.2 What policies can be effective to maximize the availability of the in-demand cybersecurity skills in the Canadian Transportation Sector?

With incidents of cyber attacks increasing at rapid pace, the need for highly-skilled professionals who are capable of anticipating and responding to these types of threats have never been greater. However, where there exists a shortage of talent, there appears to also be a widening skills gap among talent employed by transportation sectors that are operating in cybersecurity roles. Recent reports have indicated that the global cybersecurity workforce shortage is projected to increase to 3.5 million individuals by 2021[91], and in Canada, it is estimated that approximately 100,000 cybersecurity related positions need to be filled by 2023.[92] This labour market imbalance highlights the demand for a comprehensive policy framework that is geared towards expanding the existing talent pool, bolstering skills of existing employees, and creating a highly-skilled cybersecurity workforce.

Building awareness of the issues related to cybersecurity is considered to be an initial starting point, as discussed in part 2.2 of this report. A key aspect of this awareness campaign should be centred on introducing concepts of responsibility, expectations and accountability as a platform to develop the necessary skills that are required to confront cyber-related threats.[93] Similarly, creating additional training opportunities for non-cybersecurity-specific talent, such as OT engineers, traffic center operators and managers, is important. Such initiatives can contribute to further cybersecurity awareness building, knowledge sharing and transfer among staff, benefiting road authority employees whose jobs are not necessary aligned to cybersecurity. This in turn, may allow for the redeployment of these individuals into cybersecurity roles within the organization, should the need arise.

Incorporating cybersecurity into the curriculum of STEM (Science Technology Engineering and Mathematic) based subjects across the education system from the primary through to the post-secondary level is also an important policy measure This can add a multidisciplinary approach to the study of various concepts, issues and principles that are of relevance to cybersecurity. As it stands, there are initiatives that are currently being implemented in Canada which are geared towards achieving this objective. One such initiative is CyberTitan, a Canadian youth cyber education program that is administered by the Information and Communications Technology Council in collaboration with government, schools, and a number of industry stakeholders. The program's main area of focus is equipping middle and secondary school students with cybersecurity skills that are needed in today's digital economy. This is done by creating learning opportunities for students to engage in hands-on simulated environments that develop the skills essential to their transition into post-secondary ICT education pathways.[94]

Greater collaboration between transport cybersecurity professionals and the academic community is also

[90] National Cyber Strategy of the United States of America: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[91] Cybersecurity Ventures https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[92] Forecasting demand for Cybersecurity Workers in Canada, 2017-2023 https://www.ictc-ctic.ca/wp-content/uploads/2019/02/ICTC_Forecast-Cyber-security_1.31.19.pdf

[93] Cybersecurity Considerations for Public Transit: https://www.apta.com/resources/standards/Documents/APTA%20SS-ECS-RP-001-14%20RP.pdf

[94] Information and Communications Technology Council: https://www.cybertitan.ca/index.php/about/what-is-cybertitan/

another avenue that should be explored further. Specifically, subject-matter experts on cybersecurity should be invited to play an active role in the development of the curriculum of certain engineering programs - particularly those related to transportation - so as to incorporate cybersecurity as a core component.

Lastly, skilled foreign talent is an important supply stream that Canadian companies can seek to tap into as a way of bridging the existing skills gap in Canada. To this end, leveraging the existing immigration channels may prove to be a viable method of attracting and recruiting cybersecurity professionals from other countries. This can be achieved by way of targeting specific occupations that are directly related to cybersecurity - such as those identified in the previous section of this report (cybersecurity architect, cybersecurity engineer etc.).

Part 5: Recommendations and Conclusions

Based on insights gained from key informant interviews and secondary research, it appears that there are insufficient cybersecurity practices or protocols geared at road authorities to monitor and respond to cyber incidents in Canada. This is partially due to a lack of cybersecurity awareness and an over reliance on internal IT groups. Consultations with industry experts based in the U.S. and Canada complemented with comprehensive secondary research identified the need for Canadian road authorities to develop an OT cybersecurity framework, a cybersecurity risk management plan and a cybersecurity protocol for legacy system and ITS integration. Simultaneously, road authorities must also focus on the development of a cybersecurity talent and skill pipeline through methods like partnering with universities, colleges and professional development institutions in cybersecurity, to provide industry-specific cybersecurity trainings for OT professionals, implementing cybersecurity talent and skill programs and initiatives that offer integrated learning opportunities for students, as well as identifying trustworthy consulting firms that can serve as industry experts where needed.

OT Cybersecurity Framework and Cybersecurity Risk Management Plan

Road authorities should set up an OTCF that maps IT and OT assets, infrastructure and equipment, and establishes a baseline assessment of the existing OT systems and environment.

Subsequently, a cybersecurity risk management plan should be established based on the following key risk management concepts:

Step 1: Identify the nature and type of risks. For example, cyber risks related to the stealing of personal information (PI) can arise.

Step2: Evaluate the severity of risks, to identify the level of resources and interventions required.

Step 3: Shape a framework by which to evaluate how, and to what extent, risks should be mitigated according to various scenarios.

Cybersecurity Protocol for Legacy System and ITS integration

Considering the replacement cost, and system availability, it is unlikely that road authorities will replace the entire legacy system with ITS. As a result, it is crucial for road authorities to develop a cybersecurity protocol addressing implications of integrating new technologies and services into the legacy systems and infrastructure. It is also important for the cybersecurity professionals to work closely with the OT operations and field engineers to facilitate knowledge sharing and transfer.

Cybersecurity Talent and Skill Development Pipeline

Road authorities should consider the following certifications and trainings available for OT professionals, in the interest of building cybersecurity skills among existing workers:

- The Canadian Centre for Cyber Security training available through their Learning and Innovation Hub.
- The (ISC) Certified Information System Security Professional (CISSP)
- Industry-specific cybersecurity training provided by U.S. Department of Transportation

This study identified the following in-demand cybersecurity roles that Canadian road authorities should seek to source in order to ensure that road infrastructure systems are safely developed and maintained. These roles are:

- Cybersecurity Architect
- Cybersecurity Engineer
- Vulnerability Tester
- Cybersecurity Incident Analyst

Canadian road authorities should contribute to the development and implementation of initiatives and policies that are geared towards addressing the cybersecurity skills gap in Canada. These may include:

- Funding various activities that are geared towards promoting cybersecurity education and training in schools, such as CyberTitan.
- Funding programs that offer cybersecurity internship opportunities for graduate and post graduate students.
- Partnering with universities and colleges as well as professional development institutions in cybersecurity research. This will allow for greater knowledge sharing and transfer.
- Investing in and enhancing programs that build the domestic talent pipeline from primary through postsecondary education levels.
- Leveraging internationally-trained professionals with cybersecurity skills.
- Identifying reliable consulting groups that can serve as industry experts where needed.

More Region-Specific Field Research Should be Conducted

The issues surrounding the availability and quality of cybersecurity talent, along with the necessary cybersecurity frameworks required to safeguard our roadways in an increasingly interconnected world are broad. This means that different transportation authorities will possess different needs and identify different implications of these developments that are unique to their region. While this report provides an initial glimpse into this topic, further research is required at a regional (provincial/territorial) level in order to obtain a complete picture of cybersecurity needs and action plans for transportation authorities across Canada.

APPENDICES

A. Sample ITS Job Posting by Canadian Road Authorities

Job Title: Intelligent Transportation Engineer[95]

The Provincial Electrical & ITS (Intelligent Transportation Systems) Engineering department provides expert Electrical and ITS Engineering Services to HQ, Information Management Branch (IMB), Regions, Districts, and Major Projects, as well as operational support for maintaining and operating ITS devices provincially. The ITS Engineering Section develops and maintains provincial transportation ITS standards, and coordinates design and installation of Intelligent Transportation Systems (ITS), including roadway sensors, CCTV, communication networks, and Dynamic Message Signs (DMS).

The position will be responsible for identifying, and supervising the development and implementation of Intelligent Transportation System (ITS) standards that govern the design, installation, operation of Intelligent Transportation Systems. The position provides expert advice and services to the Province, IMB, Regions, Districts, and other Public Agencies regarding all ITS infrastructure and fibre-optic communication. This position must stay informed and current of the most recent developments in this professional field to ensure effective and efficient service delivery. The position requires the individual to be technically proficient, self-learning, and have excellent communication skills.

In order to be considered for this position, your application must clearly demonstrate how you meet the education, experience and professional designation requirement as outlined below:

- Bachelor’s degree in Electrical Engineering with four years of varied ITS and transportation related experience.
- Registration or eligible for registration with the Engineers and Geoscientists of BC (EGBC).
- Experience working with the following:
    - Telecommunications networks, including fibre-optics;
    - Industrial Control Systems (ICS) and instrumentation;
    - Industry grade electronics and sensors;
    - Programmable Logic Controller (PLC);
    - CCTV systems;
    - Intelligent Transportation Systems;

An equivalent combination of education and experience may be considered.

Preference may be given to applicants with any of the following: (applicants that screen in on the above essential criteria may be further screened on any of the following preferences)

- IMSA Traffic Signal certification;
- Roadway lighting and photometry;
- Information technology; and
- Computer Networking.

[95] Website accessed on February 3rd, 2019 https://bcpublicservice.hua.hrsmart.com/hr/ats/Posting/view/57443

Provisos:

- Valid Class 5 Motor Vehicle License.
- Ability and willingness to travel throughout the Province.

B. Methodology

This report was created using a variety of primary and secondary research tools. Primary research tools included a select number of key informant interviews with road authorities and cybersecurity experts working across Canada and the U.S., gaging: a) their understanding of the ITS development and potential cybersecurity risks associated to road transportation sector; b) the best cybersecurity practices and protocols for road authorities to implement; c) knowledge, skillsets, and expertise that are needed by road authorities to ensure that road infrastructure systems are evaluated, designed, deployed, and maintained; d) how Canadian road authorities currently acquire or develop the necessary cybersecurity talent; and d) what's missing in the talent/skill development process, among others.

The secondary research component of this study included a thorough literature review of cybersecurity risks commonly exist among CI sectors and unique to Canada's road transportation sector, in-demand cybersecurity roles and skills that are necessary for road authorities, and relevant research to date – both from Canadian and international sources including the U.S. and the U.K. This research was conducted to identify: a) the potential cybersecurity risks resulting from convergence of ICT and OT systems and resulting impact to Canadian road authorities; b) cybersecurity talent and skill needs for Canadian road authorities to ensure road infrastructure safety; c) how are other jurisdictions approaching the need for talent development in this area; and d) what policies can be effective to maximize the availability of the in-demand skills in Canada, among others.

This study also utilized advanced analytics to build a web scraper that extracted job profiles in Canada, Australia and the U.S., trying to identify weather self-identified cybersecurity workers within the transportation sector currently possess in-demand cybersecurity skills acknowledged by industry experts and found in secondary research. 512 self-identified transportation workers' job profiles were extracted, and an approximately 20% the profiles were randomly selected from the 512 workers, resulting in a sample of 98 workers. Job files were then analyzed via text mining and natural language processing to identify relevant skills and competencies.

A second web scraping exercise was conducted to extract job postings related to cybersecurity and transportation sector technical roles from Canadian road authorities' job posting website. This phase was abandoned as less than 10 jobs were found and they were exclusively in the railroad and private sector.

C. Limitations of research

As with all research, certain limitations can occur that may influence findings. While ICTC has attempted to mitigate these as much as possible, the following limitations exist in relation to this project.

Primary Research: limited by project budget and scope of the study, only six key informational interviews were conducted. The research findings related to how Canadian road authorities are currently acquiring cybersecurity talents are solely based on interviews with road authorities in Province of British Columbia. further research is required at a regional (provincial/territorial) level in order to obtain a complete picture of cybersecurity needs and action plans for transportation authorities across Canada.

Data Analytics: limited by project budget, web scraping exercise was only conducted once in this study (January, 2019). That said, while this exercise provided a thorough examination of whether Canadian road authorities have had necessary cybersecurity talent and skills, more frequent web scraping exercises with larger sample sizes would have been useful to more accurately capture insights on the cybersecurity talent gap among Canadian road authorities.