# The Cybersecurity Path:

## Positioning Windsor-Essex and Chatham-Kent for the Future

**Dr. Victoria Abboud** | May 2021

WE·tech ALLIANCE

INVEST WINDSOR ESSEX

# EXECUTIVE SUMMARY

Cybersecurity as a whole has become part of a louder conversation about the imperative for all citizens to be cautious with their data and how they engage in the digital world. Cybersecurity is not a new concern, of course, but the COVID-19 pandemic has induced an exponential rush to work, learn, and interact online that has brought to light the gaps in how we typically interact digitally.

With nearly a dozen sub-domains, cybersecurity is an industry that offers ample opportunity for expansion, research, and development. The Canadian national strategy for cybersecurity identifies three key themes – secure and resilient Canadian systems, an innovative and adaptive cyber ecosystem, and effective leadership and collaboration – that specify the scale and scope of a national cybersecurity interests. With the potential GDP contribution of cybersecurity (over $2.3 billion in 2018), it is clear that cybersecurity is an industry that can yield significant value for the economy.

Local researchers from the University of Windsor are devoting time and energy to automotive cybersecurity and the value and importance of cybersecurity for the automotive and automobility industries for this region. Through increased programming and opportunities at both the University of Windsor and St. Clair College, it is clear that the post-secondary education sector has taken notice of the potential.

The potential for this region is also being noticed by business leaders outside of the area as well. Companies like Vehiqilla are targeting the region as the place to locate operations because of the momentum that is building here. While "cyberpreneurship" rates are low in this region, there is ample opportunity for entrepreneurs focused on cybersecurity to set their companies locally while reaching global markets, especially with the Windsor-Detroit border as a key feature of this area.

By noting and adapting other global examples like those of Israel and Estonia, the Windsor-Essex and Chatham-Kent region can improve its focus and create an intentional path towards a future in cybersecurity.

Through active engagement and collaboration among education, government, and business, leaders can support this region to become a strong global player in the cybersecurity industry. Key recommendations generated through the research and interviews from this report include systems-level levers, research and development, skills and training, and community investment.

This report was created with the support of

OCI Where Next Happens

AVIN CONNECTED. AUTONOMOUS.

Ontario

We acknowledge the support of the Government of Canada through the Federal Economic Development Agency for Southern Ontario.

Nous reconnaissons l'appui du gouvernement du Canada à travers l'Agence fédérale de développement économique pour le Sud de l'Ontario

Canada

# TABLE OF CONTENTS


04 **Introduction**

06 **Key Considerations for Cybersecurity**
Cybersecurity in Canada
Threats and the Local Imperative

13 **Cybersecurity in Windsor-Essex and Chatham-Kent**
Regional Interest and Perspectives

17 **Anticipated Gaps and Opportunities**
Talent Shortage and Infrastructure
Automotive Cybersecurity
Cyberpreneurship and Forward Pathways

32 **Recommendations and Concluding Remarks**

34 **Resources**

39 **Acknowledgements**


# INTRODUCTION

In a time of digital transformation and the global growth in remote working, the reliance on virtual environments to conduct business, learning, healthcare, and social interaction has greatly increased. Cybersecurity as a whole has become part of a louder conversation about the imperative for all citizens to be cautious with their data and how they engage in the digital world. Cybersecurity is not a new concern, of course, but the COVID-19 pandemic has induced an exponential rush to work, learn, and interact online that has brought to light the gaps in how we typically interact digitally.

Generally speaking, "cyber security" (or "cybersecurity") refers to the "protection of digital information and the infrastructure on which it resides."[1] While traditionally cybersecurity has been imagined as the "domain of technical experts," Canada has recognized the need for all citizens to recognize their responsibilities for individual and collective cyber safety.[2] Consider, for example, that "cyber security is the convergence of people, processes and technology that comes together to protect organizations, individuals and networks from digital attacks. As a result, cyber security strategies must be created based on a multi-jurisdictional collaborative model with defined roles, functions and responsibilities as well as strategic objectives."[3]

Furthermore, cybersecurity specialist efforts range from "finding bugs in software to penetration testing using social engineering," according to John Haldeman, Information Security Architect with Information Insights.[4] Haldeman cites the analysis of internal threats, software dependency and software supply chain security, and identity authentication and verification systems as three key areas that are of great interest currently.

Even before the COVID-19 pandemic, cyber security concerns and innovations were top-of-mind for some sectors. For example, the financial services sector has been addressing cybersecurity and attacks at alarming rates. Last year, a full "86% of breaches were financially motivated, the records exposed in all breaches increased by 284 percent [and] the average cost of a breach as disclosed by public firms in 2019 was $116 million USD."[5] And Deloitte reports that "manufacturers are increasingly being targeted not just by traditional malicious actors such as hackers and cyber-criminals, but by competing companies and nations engaged in corporate espionage. Motivations range from money and revenge to competitive advantage and strategic disruption."[6] In December 2020, the Identity Theft Resource Center in the United States identified that over 300 million individuals were impacted by data breaches, a statistic focused only on breaches that were publicly reported, and, surprisingly, that represented a reduction of 66% from the year prior.[7]

---

1. Public Safety Canada. (2018). National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx
2. ibid.
3. North of 41. (2020, Spring). "Top Cyber Challenges Facing Canada: SMB Perspective." Courtesy of Jeff Musson.
4. John Haldeman. (2021, January 13). Email communication.
5. Julien Bonnay. (2020, September 17) "Five Cybersecurity Trends from 2020 – And What the Future Holds." Security: Solutions for Enabling and Assuring Business. https://www.securitymagazine.com/articles/93377-five-cybersecurity-trends-from-2020-and-what-the-future-holds
6. Deloitte. (n.d.). "Global Cyber Executive Briefing: Manufacturing." Case Studies. https://www2.deloitte.com/global/en/pages/risk/articles/Manufacturing.html
7. Identity Theft Resource Center. (2021, January 28). 2020 in Review: Data Breach Report. https://notified.idtheftcenter.org/s/2014

Now, in the midst of the pandemic, the resultant distributed workforces are creating opportunities for increased cybercrimes and are subsequently calling for increased and intentional cyber awareness. Imagine, for example, an organization of twenty (20) people that is now required to work remotely. At one time, in the office, there were internal security measures, protected servers, and an entire business infrastructure that could be protected within the walls of the office. Now, with the team working from a variety of locations, the stakes are much higher: uncertainty about the security of home Wi-Fi networks, multiple devices not necessarily carrying the same protective software as office-based computers, the potential for multiple users on one device, etc. The uncertainty factor has increased dramatically.

Under the auspices of National Defence, the Government of Canada aims to engage Canadians "to foster understanding on how to protect themselves, their families, their workplace and their devices through cyber security."[8] In fact, there are numerous resources on the Government of Canada's website[9] that provide specific information related to "cyber-healthy" practices and cyber threats in particular.

Although cybersecurity has been of far-reaching concern for many years, it seems that now, given the COVID-19 pandemic, cyber awareness has become a significant topic across sectors due to increased online and virtual activity. October is cyber security awareness month in Canada. "CSAM" for short, the month-long information push is dedicated to awareness, support, and engagement with public, private, governmental and non-governmental organizations (NGOs) to ensure that Canadians recognize the vital importance of cyber security.

In order to understand the landscape of cyber security in the Windsor-Essex and Chatham-Kent regions, WEtech Alliance, with the support of the Federal Economic Development Agency for Southern Ontario (FedDev Ontario), the Autonomous Vehicle Innovation Network, the Ontario Centre of Innovation, and Invest WindsorEssex, has undertaken an environmental scan that aims to uncover the current state of cyber security in our region. Intended as an informational guide to identify how "cyber security" is understood, engaged, and discussed in the region, this report focuses on the key interests, activities, gaps, and opportunities related to cybersecurity.[10]

8. National Defence Canada. (2020). The Maple Leaf: Stories about the Canadian Armed Forces and the Defence Team that Supports Them. https://www.canada.ca/en/department-national-defence/maple-leaf.html
9. To access the Government of Canada's National Defence website devoted to cybersecurity, please see: https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2020/10/cyber-security-awareness-month.html
10. This report is the result of research, virtual interviews, and email communications conducted from August 2020 through April 2021.

# KEY CONSIDERATIONS FOR CYBERSECURITY

In order to explore cyber security effectively, it is first necessary to clarify the context in which cyber security exists both nationally and locally. As such, this section focuses on building a shared language and conceptualization of how cyber security is discussed and explained at the national level and locally in Windsor-Essex and Chatham-Kent.

## Cybersecurity in Canada

In 2018, the Government of Canada issued its *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*.[11] The forty-page report aims to inform Canadians (and interested global stakeholders) of the potential for Canada to become a leader in cyber security. Through significant stakeholder engagement, including public consultations that resulted in over 2,000 submissions, the report merges the interests of the Ministers of Defence, Innovation, Infrastructure, Public Services, and the Treasury Board.[12]

Significantly, the national strategy names three key themes – secure and resilient Canadian systems, an innovative and adaptive cyber ecosystem, and effective leadership and collaboration[13] – that specify the scale and scope of an effort such as this and provides additional details about how Canada intends to position itself globally in the digital world. One key piece of the cybersecurity puzzle is ensuring that Canadians across the country recognize the need to "play an active role in shaping and sustaining our nation's cyber resilience."[14]

Despite the national efforts to curb cyber threats and to safeguard Canadians' data, the Canada Revenue Agency itself, in the summer of 2020, suffered a "credential stuffing attack that affected 5,500 Canadians. By using fraudulently acquired passwords and usernames of over 9,000 users worldwide, attackers "took advantage of the fact that many people reuse passwords and usernames across multiple accounts. [. . .] Affected accounts were cancelled as soon as the threat was discovered"[15] and measures were taken to complete a forensic analysis of the incidents. A month later, "the CRA identified suspicious activities occurring between early July and August 15 [2020] on approximately 48,500 of the more than 14 million CRA user accounts."[16]

11. Public Safety Canada. (2018). National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx
12. ibid, p. ii.
13. ibid, pp. 3; 12-29.
14. ibid, p. 2.
15. Government of Canada. (2020, August 15). "Statement from the Office of the Chief Information Officer of the Government of Canada on Recent Credential Stuffing Attacks." https://www.canada.ca/en/treasury-board-secretariat/news/2020/08/statement-from-the-office-of-the-chief-information-officer-of-the-government-canada-on-recent-credential-stuffing-attacks.html
16. Government of Canada. (2020, September 17). "Statement from the Office of the Chief Information Officer of the Government of Canada on Recent Cyber Attacks." https://www.canada.ca/en/treasury-board-secretariat/news/2020/09/update-from-the-office-of-the-chief-information-officer-of-the-government-canada-on-recent-cyber-attacks.html

> The Canadian cybersecurity industry contributed over $2.3 billion in GDP and 22,500 jobs to the Canadian economy in 2018.

Not only is cyber awareness necessary for national safety, but cybersecurity as a whole is also a strong economic driver. According to the International Data Corporation (IDC) Canada and the Information and Communications Technology Council (ICTC), in 2015 cybersecurity "contributed $1.7 billion to Canada's GDP and consisted of over 11,000 well-paying jobs."[17] By 2018, according to the *Statistical Overview of Canada's Cybersecurity Industry* published by Innovation, Science, and Economic Development Canada (October 2020), "the Canadian cybersecurity industry contributed over $2.3 billion in GDP and 22,500 jobs to the Canadian economy" in that year alone.[18] In 2021 and beyond, the global cybersecurity industry is expected to increase by 66% leading to thousands of additional jobs for Canadians.[19] Jeff Musson, CEO of Coding for Veterans and Entrepreneur-in-Residence and Advisor for the National Crowdfunding and Fintech Association of Canada, estimates that there are currently 4 million unfilled cybersecurity jobs globally.[20] Of course, "a global shortage of qualified professionals represents an immediate and growing opportunity for Canada's highly educated workforce."[21] Consider, also, the implications for the startup community from a talent and even larger security perspective,[22] says Noah Campbell, former Tech Community Program Manager at the WindsorEssex Economic Development Corporation (now known as Invest WindsorEssex) and WEtech Alliance. Within Canada, Ontario boasts 52% of the employment share[23] in the cybersecurity industry which could create unique and interesting opportunites for the Windsor-Essex and Chatham-Kent region.

## Threats and the Local Imperative

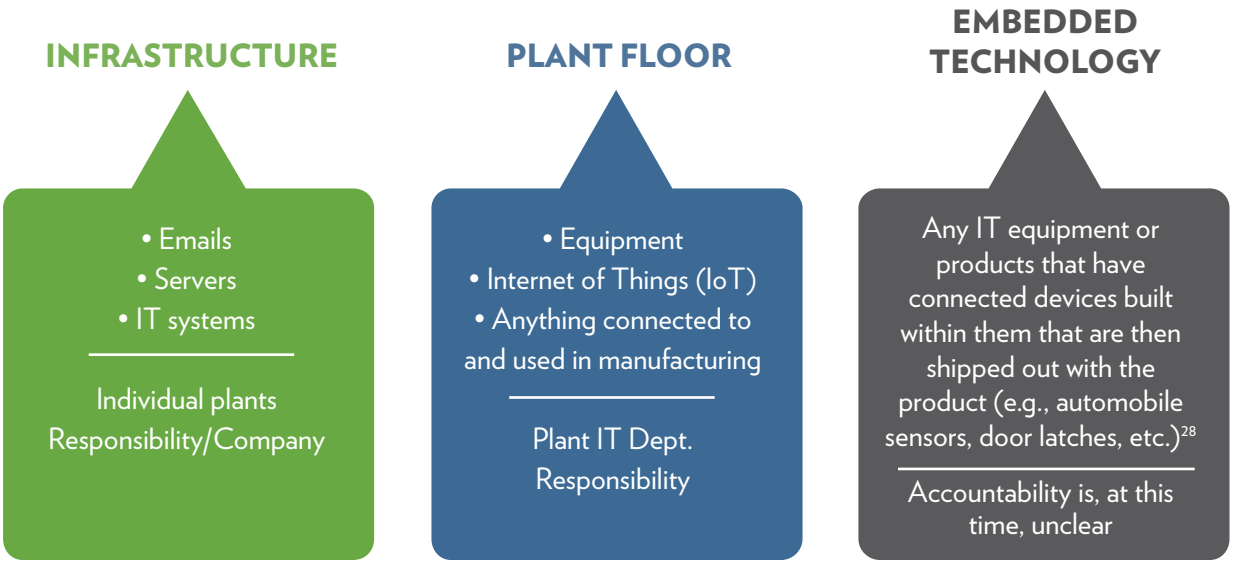
Cyber awareness, the understanding and ability to pre-empt potential criminal activity, requires a multi-pronged approach. End users themselves must be vigilant to avoid falling prey to cybercriminals, but there are also organization - and leadership-level responsibilities. In a discussion about trucking as a key targeted industry, Cristina Commendatore notes that "cybercriminals attempt to obtain businesses' data by hacking

17. International Data Corporation (IDC) Canada. (2015, December). "2016 Canadian ICT Predictions and Forecast: Digital Transformation and Disruption." (qtd. in Public Safety Canada, 2018).
18. Innovation, Science, and Economic Development Canada. (2020, October). Statistical Overview of Canada's Cybersecurity Industry in 2018. https://www.defenceandsecurity.ca/UserFiles/Uploads/publications/reports/files/document-35.pdf
19. Research and Markets. (2016, August). "Cyber Security Market – Global Forecast to 2021." (qtd. in Public Safety Canada, 2018).
20. Jeff Musson. (2020, August 25). Virtual Interview.
21. Public Safety Canada (2018), p. 20.
22. Noah Campbell. (2021, January 20). Email communication.
23. Innovation, Science, and Economic Development Canada. (2020, October). Statistical Overview of Canada's Cybersecurity Industry in 2018. https://www.defenceandsecurity.ca/UserFiles/Uploads/publications/reports/files/document-35.pdf

directly into the system through IT deficiencies and by targeting employees."[24] To combat such threats, Fortinet, an American multinational corporation devoted to cybersecurity products and services, suggests that "the first hurdle to overcome in protecting an organization's crown jewels is to bridge the gap between business leader and cybersecurity expert perceptions of what organizations need to protect."[25] In order to minimize the gap between leaders and cyber experts, local company Next Dimension launched a digital leadership workshop with CISCO that helps organizations define digital leaders and digital champions within an organization to define a digitial leadership strategy. Programs like this, suggests Brandy Coulsey, Next Dimension's Marketing and Vendor Relations Manager, "can help organizations deploy best practices and build the IT roadmap and opportunities. Every company is a technology company and cybersecurity is the most direct and concerning threat against tech. If someone attacks the power grid, then you're not up and running. Simple as that."[26]

The automotive sector is another example where cyberthreats can be highly destructive. Paul Bellack, Magna's Global CTO, identifies three areas through which manufacturing could be a prime target because of the different tiers of product development, assembly, and deployment.[27] Based on the potential vulnerabilities, accountability and protection become especially vital.

### Three Potential Target Areas in Automotive Manufacturing



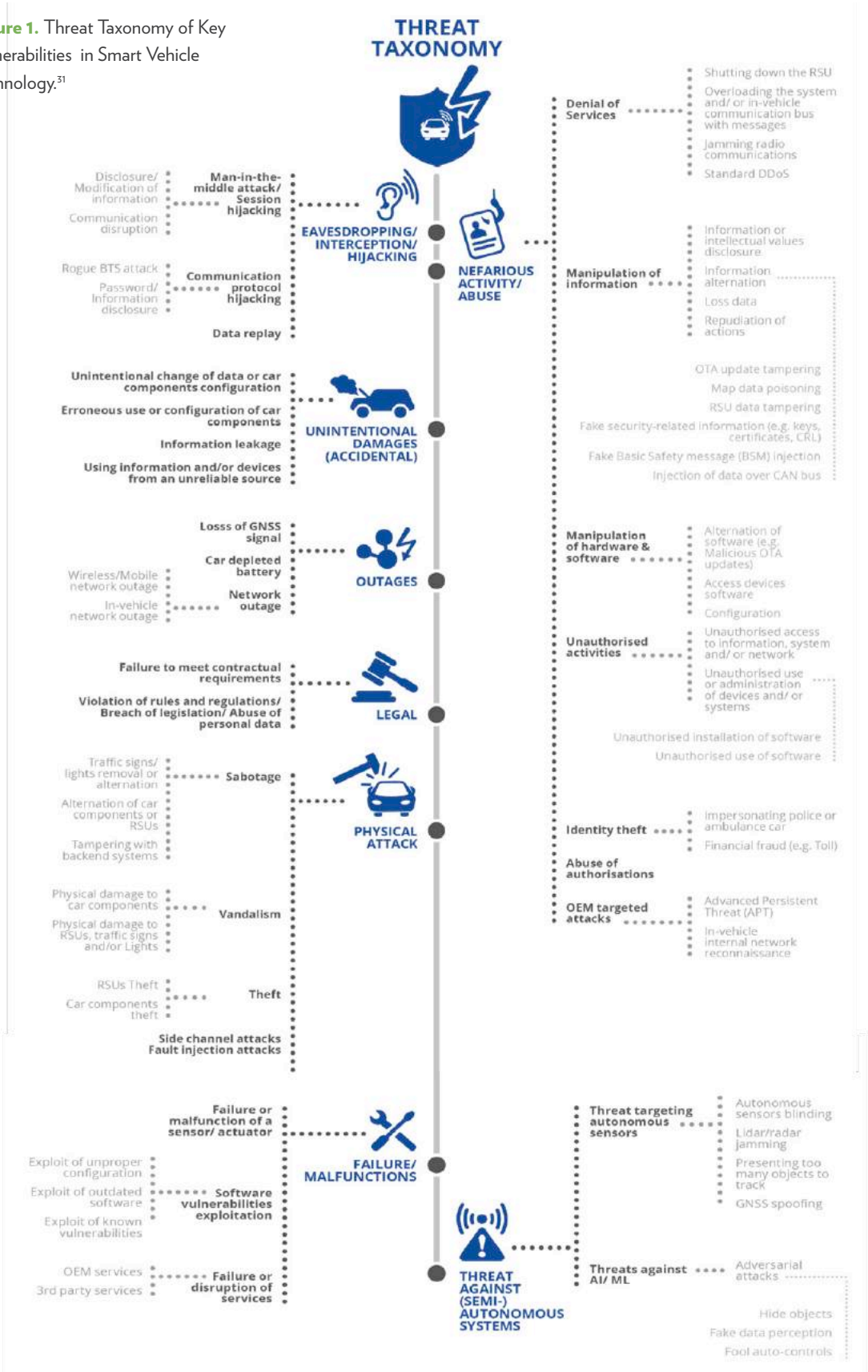

24. Commendatore, Cristina. (2020, May 12). "Trucking Remains a Top Target for Cyberattacks." Fleet Owner. https://www.fleetowner.com/covid-19-coverage/article/21131096/trucking-remains-a-top-target-for-cyberattacks
25. Fortinet. (2019, March 08). "Taking a Priority-Based Approach to Cybersecurity." BLOG. https://www.fortinet.com/blog/ciso-collective/protecting-your-companys-crown-jewels-from-cybersecurity-attack
26. Brandy Coulsey. (2020, November 19). Virtual Interview.
27. Cited by Matthew Johnson. (2020, September 16). Phone Interview.
28. ibid.

For example, if a car contains several connected components and one fails, accountability is a vital consideration. Whether responsibility is held with the parts manufacturer, the vehicle assembly line, the plant floor supervisor, or another actor in the long line of vehicle manufacturing processes, it's imperative to recognize that a cyberattack can, in fact, cause significant harm. According to BlackBerry, "many vehicle original equipment manufacturers (OEMs) do not diligently protect their products. In fact, over 60% of OEMs test less than half of their hardware and software for vulnerabilities."[29] And global players in the automotive market are taking notice.

The European Union Agency for Cybersecurity lists 11 attack scenarios related to smart vehicles, each with a cascade effect that reaches individuals, organizations, other vehicles, and entire communities. The risks are potentially devasating and can result in hackers gaining access to vehicles to travel to restricted locations, influencing car behaviours, compromising back-end servers, and even deploying malicious programs to disrupt regional traffic.[30] Figure 1, on the next page, outlines the key vulnerabilities in smart vehicle technology.

29. BlackBerry Cylance. (2020). "2020 Threat Report." https://www.blackberry.com/us/en/products/resource-center/2020-threat-report
30. European Union Agency for Cybersecurity (ENISA). (2019, November). "ENISA Good Practices for Security of Smart Cars." https://www.enisa.europa.eu/publications/smart-cars

**Figure 1.** Threat Taxonomy of Key Vulnerabilities in Smart Vehicle Technology.[31]




31. ibid.

With so many potential vulnerabilities, there is increased need for cyber awareness and advanced decision-making so that vehicles can be designed with cybersecurity in mind. Dr. Mitra Mirhassani, Associate Professor of Electrical and Computer Engineering at the University of Windsor and recent awardee of the Automotive Parts Manufacturers' Association (APMA) Institute of Automotive Cybersecurity Outstanding Individual Cyber Achievement Award, is adamant that "it doesn't matter how secure the software is. As long as the hardware or electronic parts are vulnerable to the attack points, [there is significant risk]. Even the tire pressure sensor can provide an opening for a hacker to go into the network and engage in malicious activity." Recognized as one of Canada's Top 20 Women in Cyber Security (2020) by IT World Canada, Dr. Mirhassani cautions that "our whole system – the whole interconnected system – is as strong or as weak as our weakest link. We must be careful."[32]

January 2021 marks the launch of the SHIELD Automotive Cybersecurity Centre of Excellence. Co-founded and led by the University of Windsor's Drs. Ikjot Saini and Mitra Mirhassani, SHIELD "will focus on developing the skills, innovations and policy to secure connected and autonomous vehicles."[33] Additionally, the APMA will collaborate with SHIELD "to develop market-based technologies to meet the needs of producers and consumers and build academic programs to address industry's evolving requirements."[34]

> "It doesn't matter how secure the software is. As long as the hardware or electronic parts are vulnerable to the attack points, [there is significant risk]. Even the tire pressure sensor can provide an opening for a hacker to go into the network and engage in malicious activity."
>
> DR. MITRA MIRHASSANI
> *Associate Professor of Electrical and Computer Engineering, University of Windsor*

32. Mitra Mirhassani. (2020, November 13). Virtual Interview.
33. Waddell, Dave. (2021, January 28). "University of Windsor Establishes First Canadian Transportation Cybersecurity Centre." The Windsor Star. https://windsorstar.com/news/local-news/university-of-windsor-establishes-first-canadian-transportation-cybersecurity-centre
34. ibid. For more information, please visit https://www.shieldautocybersecurity.com

With local researchers investing their expertise in identifying the key areas that the automotive industry needs to protect, and potentially how to protect those areas, attention is also being paid to supporting up-and-coming talent in the region. St. Clair College, for example, is expanding its offerings to grow cybersecurity programs. According to James Marsh, Dean of the Zekelman School of Business and Information Technology, "cybersecurity will become a big part of the automotive industry. We're focusing on cybersecurity and autonomous vehicle security. We want our graduates and community to be ready."[35]

> "Cybersecurity will become a big part of the automotive industry. We're focusing on cybersecurity and autonomous vehicle security. We want our graduates and community to be ready."
>
> JAMES MARSH, *Dean of the Zekelman School of Business and Information Technology*

While cybersecurity has been studied for many years, it seems that these COVID-influenced days of working in distributed workforces are increasing individuals' awareness of inherent threats. "The longer we stay home and exchange information in more casual ways," notes Dr. Maura Grossman of the University of Waterloo, "important information and corporate information is at much greater risk. Because so many people are glued to the Internet 24/7, including school kids, we've seen the exponential increase in the use of technology such as video conferencing and cloud-based storage. Society is rightfully looking elsewhere in the face of public health concerns, and fraudsters are taking advantage of that."[36]

35. James Marsh. (2020, September 21 and March 22). Phone Interview and Email Communication.
36. qtd. in University of Waterloo. (2020, June 03). "Cybersecurity in the Age of COVID." Waterloo Stories. https://uwaterloo.ca/stories/news/cybersecurity-age-covid

# CYBERSECURITY IN WINDSOR-ESSEX AND CHATHAM-KENT

Locally, there are several organizations and individuals that have been embedded in the cybersecurity world for years. With new research and interests coming to light frequently – the technology changes rapidly, as one would expect – it is clear that there are focused efforts related to cyber awareness and cybersecurity in Windsor-Essex and Chatham-Kent. This section highlights some of the more prominent perspectives to shed light on existing contributions and trajectories.

## Regional Interest and Perspectives

The Windsor-Essex and Chatham-Kent region hosts a number of organizations and opportunities related to cybersecurity. While many companies like Next Dimension, AlphaKOR, and Splice Digital provide training and/or services related to securing businesses' data and infrastructure, other organizations like Black Boys Code and Code Ninjas are supporting the potentional cybersecurity experts of the future. In addition, BlackBerry has partnered with the University of Windsor to deliver cybersecurity curriculum, BlackBerry Bootcamp, for graduate students in the Master's of Applied Computing program.[37]

Although not specifically devoted to cybersecurity training, Black Boys Code and Code Ninjas are supporting the learning and growth of young people who might not otherwise engage in computing or coding, and who could be enticed into careers in related fields. The Windsor chapter of Black Boys Code, for example, is led by Claudius Thomas who is the WEtech Alliance 2021 Tech Mentor of the Year. In his interview with *The Windsor Star*, Thomas lauds the surprising skill level of local youth: "We had to re-do our curriculum," he says, because "some of them were giving us Week Four projects in Week One."[38] Perhaps less surprising is that young people are already ahead of the game, so to speak, in that they are learning code and programming languages on their own while also sometimes taking advantage of more formalized opportunities to learn. In Thomas' interview, he highlights the importance for young Black students to see themselves working in tech fields: "Before you can harness a creative mind to tackle the rapidly expanding opportunities of computer coding, you have to provide the vision that it is possible."[39] And the interest continues to increase. While the first class of 8- to 12-year-olds was oversubscribed by half, Black Boys Code offered a free program in the summer of 2020 that included a section specifically for 13- to 17-year-olds.

While youth are certainly being encouraged to enter tech fields through regional and national organizations like Build A Dream, WEtech Alliance, Black Boys Code, and Code Ninjas, there are training opportunites for adults who are perhaps seeking the chance to improve their skillsets. Next Dimension, in partnership with

37. BlackBerry. (2020, May 11). "The University of Windsor and BlackBerry Partner to Educate Future Data Scientists." Media Release. https://www.blackberry.com/us/en/company/newsroom/press-releases/2020/the-university-of-windsor-and-blackberry-partner-to-educate-future-data-scientists
38. qtd. in Waddell, Dave. (2020, June 29). "Black Boys Code Establishes Windsor Chapter." The Windsor Star. https://windsorstar.com/news/local-news/
39. ibid.

KnowBe4 and Build A Dream, offers Cybersecurity Awareness Training fully online and free of charge to support "good cyber hygiene,"[40] and Palette Skills, lauched in 2017 by Arvind Gupta and AJ Tibando, offers an accelerated cybersecurity training program in partnership with The Fields Institute to train people for high-demand positions within the cybersecurity industry. According to Haley Morrison, Head of Marketing and Communications at Palette Skills, "the program focuses on working with employers and cybersecurity experts to create a curriculum that rapidly prepares participants for in-demand cybersecurity roles and increases the cybersecurity talent pools."[41]

There is strong regional interest in cybersecurity, according to Dr. Ikjot Saini, Assistant Professor in the School of Computer Science at the University of Windsor and founder of the Women in Cybersecurity (WiCyS) Windsor Student Chapter. "So many people in 2019-20, both male and female, were interested in WiCyS," she says, "and this strong support system has grown the organization into a different concept. Community members participated in events [both in-person pre-COVID and now virtually], not only students and not only women. The organization became more focused on technology – it's for everyone – rather than on gender. It's inspiring for the work we do and for the region. It's also important to note that there are 8-10 sub-domains in cybersecurity. When systems are being designed, they need to be secured."[42] With the number of sub-domains and specializations within each, it becomes more important to recognize the vastness of the cybersecurity industry and what that could mean for regional growth and economic development.

The potential for this region is being noticed by business leaders outside of the area as well. For example, AJ Khan, CEO of Vehiqilla (Burlington, ON) and Director of the Automotive Parts Manufacturers' Association (APMA) Institute of Automotive Cybersecurity, has been watching the Windsor region's automobility initiatives: "I've been engaged with Windsor in the last year [2019-20] and I saw a lot of different things happening that are interesting. With what I learned is happening here, I knew I needed to move to Windsor-Essex."[43] With access to Canada's largest Virtual Reality CAVE (cave automatic virtual environment), housed at the Invest WindsorEssex Automobility and Innovation Centre, Khan and his team (expected to grow to 50 employees in two years) can "digitally twin and test products before making them. I want to focus on cyber security in auto mobility," he says, because "the transformation of mobility is going to affect everything around us." Further, Khan is confident in Windsor's momentum: He's convinced "that Windsor is becoming the automobility capital of Canada and has the potential for a global leadership position."[44]

40. Next Dimension Academy. https://www.nextdimensioninc.com/cybersecurity-user-awareness-training/
41. Haley Morrison. (2021, March 19). Email Communication.
42. Ikjot Saini. (2020, October 02). Virtual Interview.
43. qtd. in Waddell, Dave. (2020, September 21). "Windsor Region Gaining Traction in Developing into Auto Cyber Security Hub." The Windsor Star. https://windsorstar.com/news/windsor-region-gaining-traction-in-developing-into-auto-cyber-security-hub
44. qtd. in Waddell, Dave. (2020, September 17). "Cyber Security Company Moves Headquarters to Windsor." The Windsor Star. https://windsorstar.com/news/cyber-security-company-moves-headquarters-to-windsor

> Windsor is becoming the automobility capital of Canada and has the potential for a global leadership position.
>
> AJ KHAN, *CEO of Vehiqilla and Director of the Automotive Parts Manufacturers' Association (APMA) Institute of Automotive Cybersecurity*

Attracting (or supporting local) entrepreneurs is a key lever for this region to increase the interest in the area. Windsor Works, the report commissioned by the City of Windsor to identify key opportunities for the city's future economic development, identifies the support of new businesses as an important driver: "Windsor's small businesses and new start-ups will be vital contributors of the city's future economic growth. Rather than betting on the pursuit of large corporations in order to entice them to make one major relocation decision, the city administration is favouring an approach of 'building small wins' so that future employment growth increasingly comes from attracting multiple smaller companies with [fewer] than 50 employees."[45] While the report does not identify the types of businesses, there is strong favour locally for those in the automobility sector, and, based on the research for this current cybersecurity report, there is strong potential for cybersecurity-focused entrepreneurship in this region.[46]

More specifically, businesses that support filling the unintended gaps in cybersecurity could be well suited. The unintended gaps in cybersecurity open businesses, organizations, governments, and individuals to a number of threats. The types of threats "are extremely diverse, with varying aims and a wide array of techniques. Malicious cyber actors include individual hackers and insider threats, criminal networks, nation states, terrorist organizations, and state-sponsored actors."[47] Of course, individual threats may seem relatively innocuous when positioned against large-scale concerns such as terrorism. However, the threat to individual security is real and the results can be devastating. Consider, for example, cyber criminals who access personal data through various means and steal an individual's money through bank accounts, or the group that infiltrates a small business and decimates the customer base. The consequences are vast and dire. Even global threats require local efforts and expertise.

45. Public First. (2020, December). Windsor Works: An Economic Development Strategy for the City's Future Growth. https://www.citywindsor.ca/cityhall/City-Council-Meetings/Meetings-This-Week/Documents/public%20agenda%20February%208,%202021%20special%20meeting%20with%20item%20number%20and%20footer%20with%20appendices%20reduced.pdf
46. See "Recommendations" for further details.
47. Public Safety Canada. (2018). National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx


THE THREAT TO
INDIVIDUAL SECURITY IS
REAL AND THE RESULTS
CAN BE DEVASTATING.

# ANTICIPATED GAPS AND OPPORTUNITIES

## Talent Shortage and Infrastructure

In Spring 2020, the International Information System Security Certification Consortium ((ISC)²) estimated that, globally, there were 3.12 million unfilled cybersecurity jobs (Figure 2).[48] In Canada, Policy Options Politiques recognized that "critical roles [in cybersecurity] are going unfilled, and it's expected that organizations across Canada will need to fill an estimated 8,000 additional cybersecurity positions by 2021."[49]

The global gap in the cybersecurity workforce varies by region, as seen in Figure 2 (below).

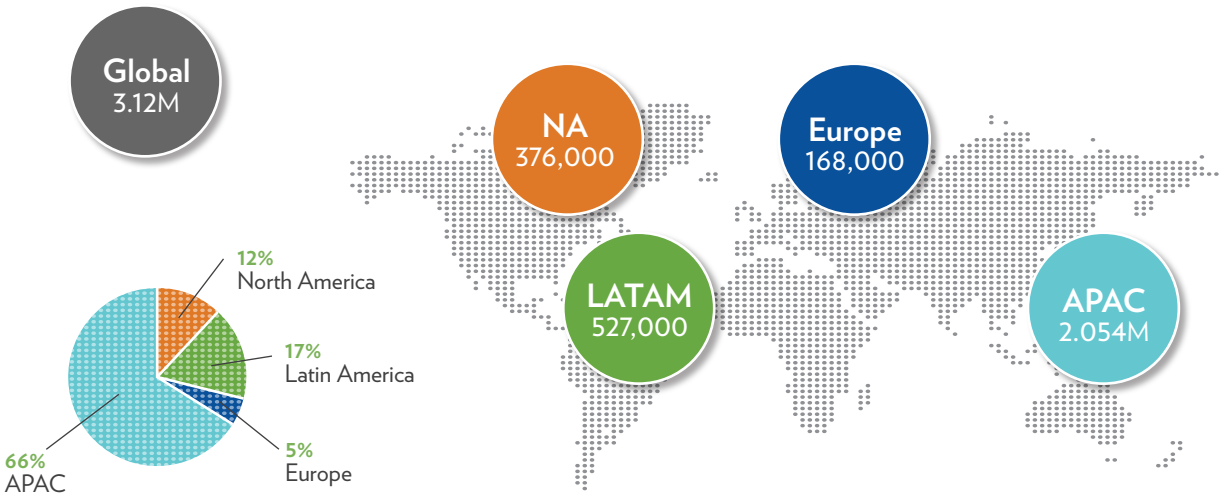



**Figure 2.** Global Cybersecurity Workforce Gap by Region.[50]

48. International Information System Security Certification Consortium. (2020). (ISC)² Cybersecurity Workforce Study. https://www.isc2.org/Research/Workforce-Study#
49. Rashotte, Rob. (2019, July 04). "The Critical Shortage of Cybersecurity Expertise." Policy Options Politiques. https://policyoptions.irpp.org/fr/magazines/july-2019/the-critical-shortage-of-cybersecurity-expertise/
50. International Information System Security Certification Consortium. (2020). (ISC)² Cybersecurity Workforce Study. https://www.isc2.org/Research/Workforce-Study#

> Part of Catalyst's goal is to be a Canadian centre for excellence in cybersecurity. Part of that goal requires expansion outside the GTA into the two key border regions: Windsor-Essex and Niagara. Manufacturing and cybersecurity go hand-in-hand.
>
> REA NERO
>
> *Project Lead, Rogers Cybersecure Catalyst at Ryerson University*

According to Indeed Hiring Lab, "[s]earches for cybersecurity positions as a share of Canadian job search activity grew 16% from 2015 to 2018. Yet even though cybersecurity searches are on the rise, they don't come close to meeting employer demand – cybersecurity's share of Canadian search activity in December 2018 was still less than a fifth of the field's share of posting activity. [. . .] The gap in cybersecurity job search rates relative to job postings suggests employers may find it difficult to recruit qualified staff. In addition, alternative gauges of job seeker interest, like the average number of clicks per posting, also indicate cybersecurity may be seeing fewer applicants than other fields."[51] Reflected another way, cybersecurity has a 0% unemployment rate in Canada which is driving the Rogers Cybersecure Catalyst at Ryerson University. Rea Nero, Project Lead for the Catalyst, indicates that part of Catalyst's goal "is to be a Canadian centre for excellence in cybersecurity. Part of that goal requires expansion outside the GTA into the two key border regions: Windsor-Essex and Niagara. Manufacturing and cybersecurity go hand-in-hand," she says.[52]

This perceived mismatch of need and talent begs the question of how Windsor-Essex and Chatham-Kent might begin to fill the gap. According to the experts and leaders interviewed for this report, our region simply does not have enough skilled talent and we do not currently have the capacity to meet the needs. "We have many of the right people,"[53] confirms Jeff Musson, but "we're missing the active engagement. What's missing is the right way of communicating. Since we're all virtual now," he says, "we can easily involve people." And Dr. Ikjot Saini reminds us that our regional ability to advance cybersecurity is not only about having the right

51. Al-Bernard, Brendon. (2019, February 14). "Canadians Increasingly Looking at Cybersecurity Roles, But It's Still a Job Seeker's Market." Indeed Hiring Lab. BLOG. http://blog.indeed.ca/2019/02/19/cybersecurity-roles-canada/
52. Rea Nero. (2020, November 09). Virtual Interview.
53. Jeff Musson. (2020, August 25). Virtual Interview.

# CYBERSECURITY HAS A 0% UNEMPLOYMENT RATE IN CANADA

people as needed in this specific moment: "We don't have enough [support and expertise] to help the skilled people go forward. You don't want to be the only expert in the region. We're missing a pipeline."[54] The ability to advance in any field requires expertise and the supports and opportunities that will allow those experts to innovate further, to ensure that the field is not simply responding or reacting to current circumstances. Especially in a field like cybersecurity, with several sub-domains, it's necessary for the region to have a strong mix of experts so that they can help move the field beyond where it currently stands.

One way to envision the potential relates to our regional strength as a border city. In 2018, the overall Canadian cybersecurity exports totalled $1.1 billion, with the lion's share -- a full 72% -- being exported to the United States. The export intensity for cybersecurity specifically, according to Innovation, Science, and Economic Development Canada, "was 3x higher compared to the Canadian ICT [information and communications technology] average."[55] This represents a large opening that would offer ample opportunity for business and talent to move between the borders in ways that benefit all involved.

> "Our regional ability to advance cybersecurity is not only about having the right people as needed in this specific moment: We don't have enough [support and expertise] to help the skilled people go forward. You don't want to be the only expert in the region. We're missing a pipeline."
>
> DR. IKJOT SAINI
>
> *Assistant Professor, School of Computer Science, University of Windsor*

54. Ikjot Saini. (2020, October 02). Virtual Interview.
55. Innovation, Science, and Economic Development Canada. (2020, October). Statistical Overview of Canada's Cybersecurity Industry in 2018. https://www.defenceandsecurity.ca/UserFiles/Uploads/publications/reports/files/document-35.pdf

The future of the region, whether focused on automotive cybersecurity or a broader perspective based on other services and operations related to cybersecurity, requires a robust talent pipeline. In order to ensure that talent are ready and well equipped to lead this region into a cybersecure future, both St. Clair College and the University of Windsor are striving to fill the educational needs of prospective talent and to identify areas of opportunity. Similarly, local organizations like Next Dimension, AlphaKOR, and Splice Digital are consistently educating their clients and offering training opportunities.

In the last 5 years, Ontario has seen an upward trend resulting in 9 colleges now offering cybersecurity programs. Locally, St. Clair College is progressing similarly. Although the college now offers a few courses and programs that address cybersecurity, James Marsh, Dean of the Zekelman School of Business and Information Technology, highlights the need for a more focused program, likely 2-3 years in duration, that would include some courses focused on automotive cybersecurity specifically. He notes that there is a significant international student population seeking several seats if the program is developed. As a "hot and up-and-coming area," Marsh notes, St. Clair could be welcoming approximately 150 students per year with total enrollment of 600 for a program like this. In addition, the college is nimble and could be collaborating closely with industry to ensure that graduates are trained in the ways most necessary for the region.[56]

The challenges in securing cybersecurity talent specifically, according to Doug Sartori, CEO and Principal Consultant of Parallel 42 Systems, is "similar to the tech gaps locally. [The lack of awareness and seeming lack of local talent] represent a barrier to investment and to successful execution of businesses. If you were launching a startup and you're focused on software, where are you going to find the resources that you need to secure your infrastructure?"[57] Given the "historically shallow talent pool locally," Sartori notes, it's important to ensure that skills are being developed here. That's why programs like that of St. Clair College are important: the College "rightly implemented a data and analytics program in the last few years in response to a real need in the community." [58]

At the University of Windsor, there have been significant strategic moves towards building capacity in cybersecurity. Although the institution currently offers a specialization in network and security for its honours undergraduate Computer Science degrees, Dr. Ziad Kobti, Director of the School of Computer Science, notes that there has been significant investment in bolstering the offerings and the research and innovation capacities of the institution. More specifically, the School objective includes "supporting industry, enhancing current offerings, creating new offerings in specific sub-domains of cybersecurity, and designing community programs. The idea is to offer research and learning opportunities that meet the range of needs from basic cyber awareness for citizens, to intensive, funded innovation and research for top-notch researchers who

56. James Marsh. (2020, September 21). Phone Interview.
57. Doug Sartori. (2021, January 11). Virtual Interview.
58. ibid.

work with the latest and greatest tools. In essence, we're creating a broad spectrum: from public outreach to advanced research and innovation."[59]

In May 2020, students from the university's Master of Applied Computing program were part of a 10-week -long virtual program, the first partnership of its kind between BlackBerry Ltd. and a Canadian university.[60] According to Neelam Sandhu, BlackBerry's vice-president of business operations and strategic accounts, "the university has a lot of tech talent. A pool of talent that's attracting a lot of tech companies to the market. [. . .] Providing students with more cyber security skills at a time when they'll be entering a wounded economy will help them maximize their economic potential, but will also protect communities trying to recover."[61]

In another first, the university's Odette School of Business has partnered with the University of Dallas' Satish and Yasmin Gupta College of Business, designated by the US National Security Agency and the US Department of Homeland Security to offer MBA and Master of Management graduates a chance "to gain internationally recognized cybersecurity skills and certification entirely online."[62] According to Kent Walker, the Odette MBA program director, "the key benefit for Canadian students is that there are very few similar programs offered in Canada, one of which can be completed entirely online. This education gap exists despite the fact that the area of cybersecurity has grown tremendously, with the trend drastically accelerated because of changes related to COVID. Our students will have an opportunity to acquire a piece of their education that is very much in demand, but not available to many other Canadians."[63]

When imagining the utility of varied programs for different levels of cyber education, consider, for example, Deloitte's guide for C-suite and boards to assess an organization's cyber risk. Through the guide and questionnaire, organizations can determine whether they have the right leader(s) and organizational talent. According to Deloitte, "A high maturity cyber security leader has the right mix of technical and business acumen to understand how the organization operates, engage with the business and know where to prioritize efforts. Teams of passionate and energized staff keep up-to-date on the latest cyber security trends, threats, and implications for their business. Cyber risk discussions are elevated to the board and C-suite level [and] there is a sufficient number of skilled staff with relevant industry experience focused on the right areas."[64] At all levels of an organization, cybersecurity becomes part and parcel of its daily operations and efforts. Much like the need for creating a region that is comprised of a strong mix of experts, leaders, and practitioners, any organization requires a balanced team to ensure that cyber risks are minimized.

---

59. Ziad Kobti. (2021, January 07). Virtual Interview.
60. Dave Waddell. (2020, May 11). "University Partners with BlackBerry to Create New Cyber Security Programme." The Windsor Star. https://windsorstar.com/61. news/local-news/university-partners-with-blackberry-to-create-new-cyber-security-programme
61. ibid.
62. "Partnership with Leading U.S. University to Offer Cyber Security Specialty to Odette Grads." (2020, September 21). University of Windsor Daily News. https://www.uwindsor.ca/dailynews/2020-09-21/partnership-leading-us-university-offer-cyber-security-specialty-odette-grads
63. ibid.
64. The full questionnaire and guide can be downloaded from Marc MacKinnon and Nick Galletto. (n.d.) "Cybersecurity: Everybody's Imperative." Deloitte. https://www2.deloitte.com/ca/en/pages/risk/articles/cyber-security-everybody-imperative.html

Of course, to build capacity regionally, it would be necessary to create pathways and collaborations. Currently, some exist, but they are not necessarily linked directly to cybersecurity. Organizations like Palette Skills, for example, support industry by creating training and internship opportunities. As part of the Government of Canada's Sectoral Initiatives Program, Palette Skills strives "to meet the needs of Canada's most innovative companies by rapidly upskilling workers."[65] With their intensive training models that require participants to have advanced math skills, Ann Lockhart, Cybersecurity Program Manager, highlights that "after 5 weeks of training and 3 weeks of project work, participants are employable by the end of the program. Often, our participants are graduates with Masters and PhD degrees, so they are well equipped to take on complex challenges. The final project they complete is the next generation of what companies are seeking."[66] And Carly Shenfeld, Palette Skills' Operations Lead, notes that the organization is "exploring specialization streaming options for their next cohort which would allow Palette Skills to accept participants with an even wider variety of [academic and professional] backgrounds."[67] Currently, Palette Skills is engaging the Windsor area to help upskill talent to fill gaps.

As is clear from the Canadian National Cybersecurity Strategy, there is appetite for advancing research and development in cybersecurity. While the national conversation highlights that "the federal government is aiming for national cybersecurity excellence," there is also recognition that such a goal "will involve enhancing and growing cybersecurity capabilities in government and industry." Divided into three categories – experimental development, applied research, and basic research – Canadian cybersecurity R&D (research and development) investment topped "close to $260 million" in 2018 and "over 90% of the R&D performed by the cybersecurity industry was funded by the industry" itself, again representing "3x more intensity than the total Canadian ICT industry average."[68] The Canadian National Cybersecurity Strategy also acknowledges that "private sector leaders will have a central role to play, as a collaborative effort is needed to ensure that all Canadians are as equipped as possible to prevent and respond to cyber threats."[69] The challenge not identified in a national-level strategy is that regional efforts require an influx of funding, supports, and capacity-building in order for such "collaborative effort" to occur.

Frank Abbruzzese, CEO of AlphaKOR Group, notes that "one organization cannot create a cybersecurity region alone. We would need to bring academia and industry together with someone like AJ Khan [of Vehiqilla], pull in two dozen key organizations who are going to build the regional model [for automotive cybersecurity, for example] and go from there."[70] The requirement of collaboration and intentional

65. Carly Shenfeld. (2020, November 24). Email Communication.
66. Ann Lockhart. (2020, November 23). Virtual Interview.
67. Carly Shenfeld. (2021, February 04). Email communication.
68. Innovation, Science, and Economic Development Canada. (2020, October). Statistical Overview of Canada's Cybersecurity Industry in 2018. https://www.defenceandsecurity.ca/UserFiles/Uploads/publications/reports/files/document-35.pdf
69. Public Safety Canada. (2018). National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx
70. Frank Abbruzzese. (2020, November 24). Virtual Interview.

> One organization cannot create a cybersecurity region alone. We would need to bring academia and industry together with someone like AJ Khan [of Vehiqilla], pull in two dozen key organizations who are going to build the regional model [for automotive cybersecurity, for example] and go from there.
>
> FRANK ABBRUZZESE, *CEO of AlphaKOR Group*

developmental strategy cannot be understated. Consider the Waterloo Region as an example. According to Dr. Ikjot Saini, "even though Waterloo currently has the two best companies for auto cybersecurity, it is not considered a specifically 'cybersecurity' region. It's one thing to have industry focus on it, but we need to think as a region: academia, students, industry, not-for-profit organizations need to sit together to determine how we can excel in this area."[71]

Arguably, there is already strong activity and collaboration among academia, industry, and the private and not-for-profit sectors, but the collaborations focus on a wide variety of industries and interests. The connections among sectors in this region have a long history. More recently, there is growing momentum and a strategic angle for this region's development as an "automotive cybersecurity" hub, but any hopes to build a region focused on cybersecurity excellence would need those collaborations to continue, and new ones to be formed, with that goal in mind.

Further, one of the key recommendations of the Windsor Works report includes a municipal "'Windsor Talent' steering group, chaired by the Mayor" that would be comprised of high-level representatives from post-secondary, K-12, Invest WindsorEssex and other "major employers in the region."[72] The committee, according to the report, would convene to make decisions and influence local educational pursuits that would address the talent challenges of the community.

---

71. Ikjot Saini. (2020, October 02). Virtual Interview.
72. Public First. (2020, December). Windsor Works: An Economic Development Strategy for the City's Future Growth. https://www.citywindsor.ca/cityhall/City-Council-Meetings/Meetings-This-Week/Documents/public%20agenda%20February%208,%202021%20special%20meeting%20with%20item%20number%20and%20footer%20with%20appendices%20reduced.pdf

## Automotive Cybersecurity

Given the region's automotive and related manufacturing history, many researchers and leaders have focused on automotive cybersecurity as the next logical evolution. In fact, the Windsor-Essex location quotient[73] for automobility is 50% larger than any other region in Canada.[74]

While cybersecurity can, of course, correlate to countless other industries such as agriculture, for example, there is a strong emphasis on supporting a regional transition to automotive cybersecurity. Ranging from connected and autonomous vehicles (CAVs) to the development of cybersafe sensors and minute componentry needed for auto manufacturing, the field of automotive cybersecurity is vast and opens a broad channel for regional focus. Figure 3, below, depicts the interconnections of the automotive and mobility ecosystem, of which automotive cybersecurity specifically is one small (but large in and of itself) component.

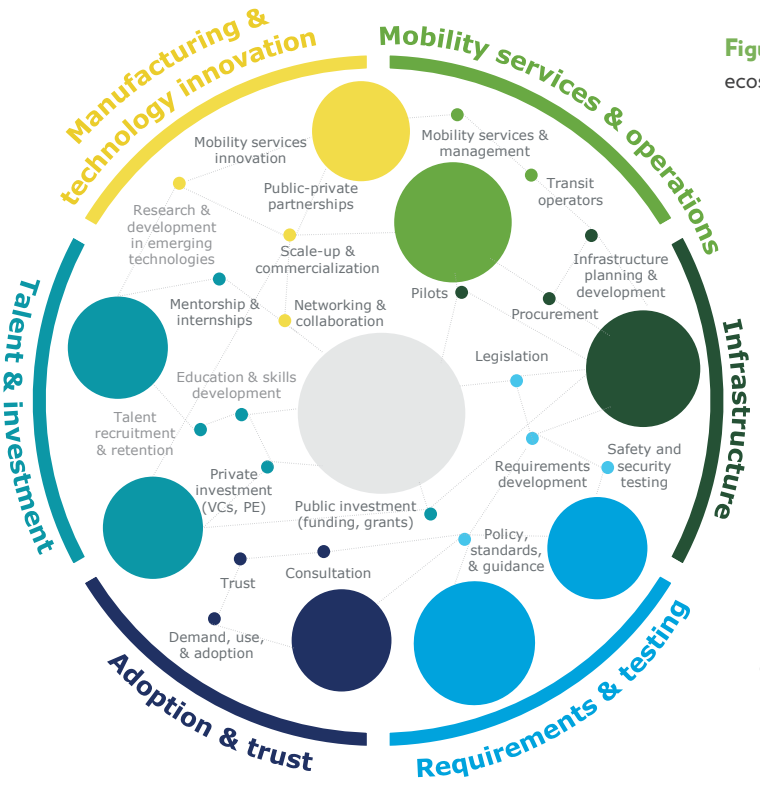



**Figure 3.** Automotive and mobility ecosystem stakeholders.[75]

While cyber attacks on vehicles are often imagined as the actual hijacking of a vehicle by a hacker, there are myriad ways that any vehicle can be attacked: "modern vehicle[s are] complex machines with over 20,000 suppliers [which] means that understanding the risks to the components from these suppliers, [to] the integration of these components, and to the entire supplier chain is a major challenge."[76] Figure 4 (next page) depicts some of the key areas of a vehicle that are under threat.

73. The "location quotient" refers to a measurement of a region's industrial specialization relative to a larger geographic unit.
74. Institute for Border Logistics and Security. (n.d.). "An Overview and Windsor-Essex's Regional Strategy on Automotive Cybersecurity." Unpublished manuscript. Courtesy of Matthew Johnson.
75. Deloitte and AVIN. (October 2020). "AVIN Ecosystem Analysis and Roadmap 2020." https://oce-ontario.org/docs/default-source/publications/fy2018-2019-oce-avin-annual-report_final-(2019-06-28).pdf?sfvrsn=2
76. A.J. Khan. (2020, April 29). "ISO21434: Understanding Risks is Key to Ensuring Cybersecurity in CAVs." LinkedIn. https://www.linkedin.com/pulse/iso21434-understanding-risks-key-ensuring-cavs-aj-khan?trk=public_profile_article_view

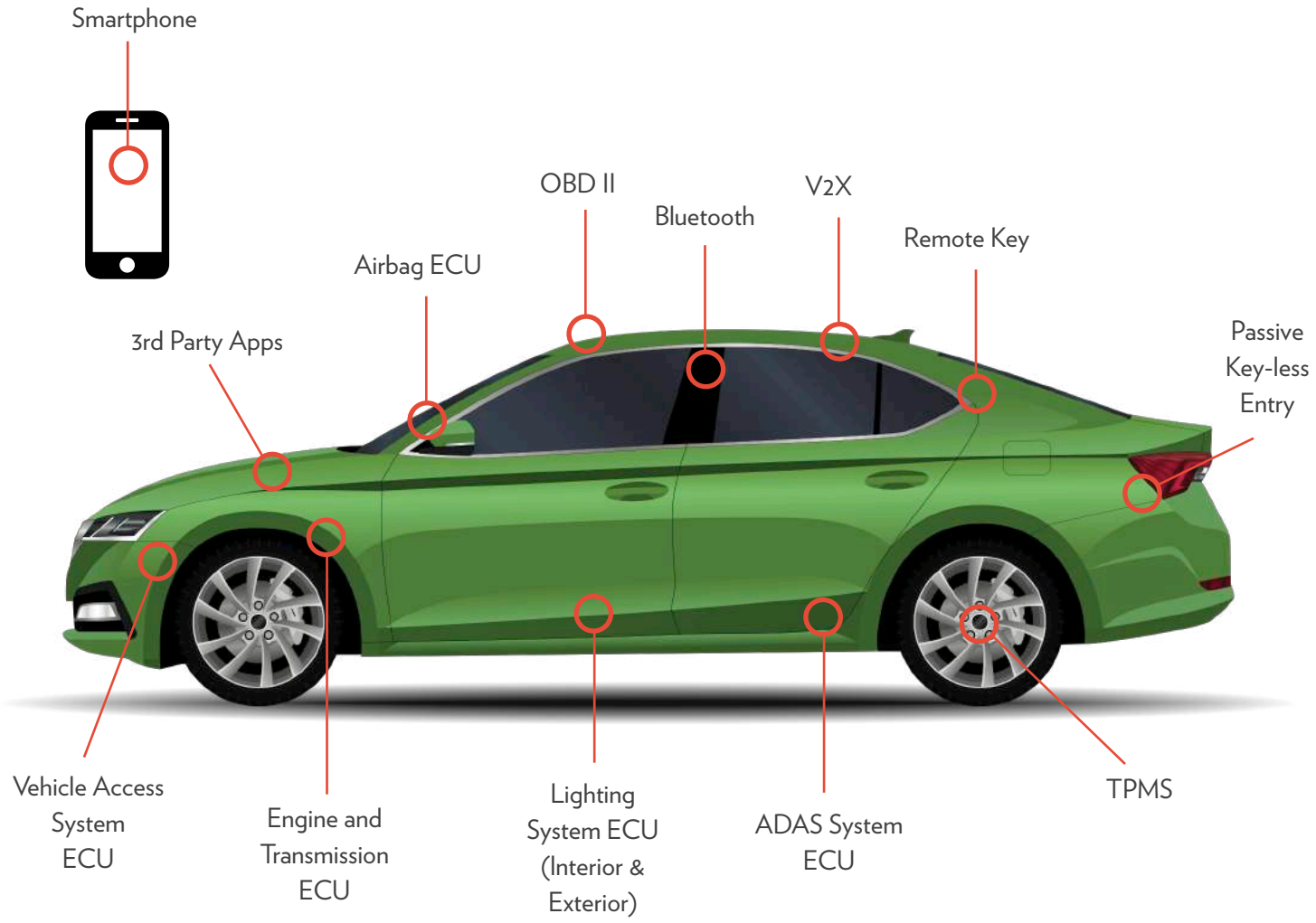



**Figure 4.** Depiction of connected/autonomous vehicle systems that could be targeted in a cyber attack.[77]

One way to secure CAVs is by creating a digital twin. The digital twin could "be programmed to flag any maintenance or service issue that arises from periodic usage or an accident. [It] will alert the OEMs' [original equipment manufacturers'] service platform via Cloud about, say, an engine part change. The OEMs can then update the vehicle owner about [the change] as well as a parts vendor" to enhance the customer experience while reducing risk.[78] Notably, Tesla's 2015 Model S launched an "operating system [that] is updated remotely with no need for the driver to visit a dealership. Instead, new features and safety updates are automatically sent to the system, and drivers are notified via an on-screen message."[79] Today, Tesla vehicles "regularly

77. Vehiqilla. 2020. https://vehiqilla.com/
78. Amar Bhosale and Sanyam Agarwal. (2020, October 16). "Cyber Security, Digital Twin, and Trusted Mobility." Telematics Wire. https://www.telematicswire.net/cyber-security-digital-twin-and-trusted-mobility-by-securethings
79. Kelsey Sakamoto. (2015). "How Tesla Plans to Lead the Connect Care Experience." Car Throttle. https://www.carthrottle.com/post/how-tesla-plans-to-lead-the-connected-car-experience/

receive over-the-air software updates that add new features and enhance existing ones over Wi-Fi"[80] which begs the question of how secure these vehicles can be given the "over-the-air" updates.

And considering that the modern car has "over 200 million lines of code," security of both vehicles themselves and any digital twins will require fail-safe measures and extensive preventative measures.[81] In order to address the potential risks, it is vital that the region ensure there is appropriate and significant regional infrastructure and expertise to safeguard our systems and citizens. Of course, the safety of citizens and data is not only a regional concern. As part of the Deloitte-OCE (Ontario Centres of Excellence[82]) investigation about CAVs (September 2019), "Canadian Government authorities have signaled that they may need to play a larger role in enforcement or auditing against privacy and security requirements in the context of emerging technologies like CAVs, and have invited stakeholders to work together on developing future policy frameworks and guidance."[83]

Consider the fact that Windsor-Essex hosts "the nation's busiest commercial border crossing [and] handles one-third of all trade between Canada and the United States. [. . .] With 4 border crossing points in Windsor-Detroit and a 5th coming in 2024, there are an estimated 5.8 million trucks that cross the Canada-US border annually.[84] Although this region has not yet encountered swathes of connected and autonomous trucks, the trucks themselves and the companies that handle the logistics of product movement are at risk. According to Mark Murrell, "trucking is a high dollar business. That means companies have relatively large amounts of cash or credit available, and they're used to paying pretty big bills. If you successfully execute a ransomware attack, you can extract a higher payment than you'd get targeting small and midsize companies in other, lower dollar industries."[85] Arguably, a cyberattack focused on trucking logistics could hamper or even immobilize the economic system that crosses the Windsor-Detroit border each day. Murrell further points out that "trucking companies typically have weak information technology (IT) policies and management [because] [. . .] when compared to driver and road safety, cybersecurity isn't a top concern."

Another consideration for automotive cybersecurity is that data has been commodified in recent years. Vehicles have become mobile data sets. Dr. Mitra Mirhassani predicts that, in the future, "auto manufacturers will sell data more than actual cars."[86] In order to ensure the safety and security of citizens and communities, it is vital to recognize that "authentication and trust will be key challenges across the CAV ecosystem and that

80. Tesla. (2021). "Software Updates." Tesla Support. https://www.tesla.com/support/software-updates
81. Institute for Border Logistics and Security. (n.d.). "An Overview of Windsor-Essex's Regional Strategy on Automotive Cybersecurity." Unpublished manuscript. Courtesy of Matthew Johnson.
82. In 2021, Ontario Centres of Excellence (OCE) changed its name to the Ontario Centre of Innovation (OCI).
83. Deloitte and OCE. (September 2019). "Cybersecurity for Connected and Autonomous Vehicles." https://www.oce-ontario.org/docs/default-source/publications/oce-apma-deloitte_cav-cybersecurity-report_sept-2019.pdf?sfvrsn=2
84. "The Epicentre of International Logistics in North America." 2016-2020. WindsorEssex Economic Development (WEEDC). http://choosewindsoressex.com/transportation. WEEDC is now known as Invest WindsorEssex.
85. qtd. in Commendatore, Cristina. (2020, May 12). "Trucking Remains a Top Target for Cyberattacks." FleetOwner. https://www.fleetowner.com/covid-19-coverage/article/21131096/trucking-remains-a-top-target-for-cyberattacks
86. Mitra Mirhassani. (2020, November 13). Virtual Interview.

the entire extended security perimeter must be considered, with a focus on cloud security, in-vehicle security, and network security. Considerations around standardization, collaboration, training and trust add complexity to being able to respond to and manage CAV cybersecurity risks."[87]

Part of the regional progression towards automotive and smart mobility innovation includes work led by Ontario's Autonomous Vehicle Innovation Network (AVIN), through the Ontario Centre of Innovation (OCI).[88] According to the AVIN website, "AVIN harnesses the capacity of Ontario's ecosystem and drives the commercialization of advanced automotive and smart mobility technologies through research and development (R&D) funding, support for talent development, and business and technical supports through its six Regional Technology Development Sites (RTDS) across the province."[89] Windsor-Essex is one such RTDS in this network, comprised of Invest WindsorEssex in collaboration with the University of Windsor, St. Clair College, the City of Windsor and WEtech Alliance, and focuses specifically on cybersecurity and cross-border technologies.

AVIN serves as a focal point for all stakeholders across the province, acts as a bridge for collaborative partnerships, and drives public education, research, analysis, and thought leadership activities to push the sector forward. To support the sector's transition to the future, AVIN is currently developing a strategy outlining current and emerging skills gaps and identifying opportunities to support the sector's workforce as it plans for the future.[90] According to Kat Tyrell, Skills and Talent Lead of Automotive and Mobility Innovation at OCI, "this work looks at multiple segments of the sector including connected and autonomous vehicles (CAVs), auto and parts manufacturing, aftermarket, transit, goods movement, and infrastructure, among others."[91] In a separate effort, Deloitte (2020) conducted a comprehensive assessment of the automotive and mobility sector, the results of which have been published in the *AVIN Ecosystem Analysis and Roadmap.*[92]

87. Deloitte and OCE. (September 2019). "Cybersecurity for Connected and Autonomous Vehicles." https://www.oce-ontario.org/docs/default-source/publications/oce-apma-deloitte_cav-cybersecurity-report_sept-2019.pdf?sfvrsn=2
88. Before 2021, the Ontario Centre of Innovation (OCI) was known as Ontario Centres of Excellence (OCE).
89. AVIN Ontario. (2020). https://www.avinhub.ca/about/
90. Kat Tyrell. (2020, November 10). Virtual Interview.
91. Kat Tyrell. (2021, March 02). Email Communication.
92. Deloitte. (October 2020). "AVIN Ecosystem Analysis and Roadmap 2020." https://oce-ontario.org/docs/default-source/publications/fy2018-2019-oce-avin-annual-report_final-(2019-06-28).pdf?sfvrsn=2

## Cyberpreneurship and Forward Pathways

Windsor-Essex and Chatham-Kent are home to numerous entrepreneurs and small- to medium-sized enterprises (SMEs) that were built here, sourced talent here, grew here, and continue to support communities here. In this seemingly global push for cyber awareness and intentional cyber security efforts, it is natural to urge entrepreneurs to devote their energies to cybersecurity broadly speaking. Given the onset of automotive cybersecurity and the ostensible likelihood that this region is moving into the automobility era, a particular group of entrepreneurs is needed. Known as "cyberpreneurs," this group of business-minded and forward-thinking individuals has a unique opportunity to develop products, services, and companies in this region that could meet global demand.

According to Dr. Ikjot Saini, "our potential is in automotive cybersecurity. We need people who can come with new ideas and we need to push them to their best. The innovation pipeline in legacy systems like General Motors and Ford are not typically as fast. Startups and cyberpreneurs can move us forward quickly."[93] And Raed Kadri, Head of Ontario's AVIN, encourages a similar regional focus: "The key is that we need everyone to work in the same direction. By drawing ideas from post-secondary education and helping our talent stay in the region, companies will have the opportunity to diversify. Windsor should be the automotive cybersecurity hub. All we need is focus."[94]

> "The key is that we need everyone to work in the same direction. By drawing ideas from post-secondary education and helping our talent stay in the region, companies will have the opportunity to diversify. Windsor should be the automotive cybersecurity hub. All we need is focus."
>
> RAED KADRI, *Head of Ontario's AVIN*

93. Ikjot Saini. (2020, October 02). Virtual Interview.
94. Raed Kadri. (2020, November 16). Virtual Interview.

Invest WindsorEssex lists eight potential cybersecurity partners from the private sector. Interestingly, only two, namely, Next Dimension and AlphaKOR, are local businesses, which suggests ample opportunity for cyberpreneurs to find and make their mark in the Windsor-Essex and Chatham-Kent region.[95] The opportunity is ripe and Brian Hendel, president of Splice Digital, sees it everywhere. A local software development company with global reach, Splice Digital typically builds technology for other companies. For any company, the opportunity lies with the talent it can secure. According to Hendel, "it's easier to shine here and get attention since the region is not yet considered a major hub." And maybe it doesn't need to be, he says, because "cybersecurity should be talked about everywhere with everyone, not just here in this region."[96]

Most, if not all, businesses need access to cybersecurity expertise to safeguard their products, services, and customers. Arguably, "business leaders simply cannot set priorities, goals, and budgets without information and advice from their cybersecurity experts. Cybersecurity leaders need business executive understanding and buy-in to be effective in their roles. Although business and cybersecurity leaders respect each other's distinctive roles, neither performs their work in a silo."[97] That interconnectedness – cybersecurity expertise and business operations – is far-reaching and offers much space for cyberpreneurs to create new offerings. With local tech startup support like the University of Windsor's EPICentre, St. Clair College's Genesis Entrepreneurship Centre, and WEtech Alliance, and local organizations focused on regional development like Connecting Windsor-Essex, Workforce WindsorEssex, and the Automotive Security Research Group's Windsor Chapter, cybersecurity could be the focal point for regional growth.

Creating any new business comes with its challenges, of course. And cybersecurity is no different. Except, perhaps, that one challenge identified specifically for cyberpreneurs, according to Kevin Magee, Chief Security and Compliance Officer at Microsoft Canada, includes "founders selling startups too early or building what ultimately becomes a feature of someone else's product rather than a world-changing company in its own right."[98] In addition, as Stefan Palios of Betakit notes, in the highly technical world of cybersecurity, there is a "language barrier" because "the in-depth research [that cybersecurity] is based upon can be difficult to explain, and many cyber innovators lack experience in contextualizing their innovations to outsiders. When you don't know the lingo, it can be hard to connect."[99] The barriers, however, need not stop the momentum in this region. With broad-scale collaboration and skill-building, there is still opportunity for the Windsor-Essex and Chatham-Kent region.

---

95. Institute for Border Logistics and Security. (n.d.). "An Overview and Windsor-Essex's Regional Strategy on Automotive Cybersecurity." Unpublished manuscript. Courtesy of Matthew Johnson.
96. Brian Hendel. (2020, December 16). Virtual Interview.
97. Fortinet. (2019, March 08). "Taking a Priority-Based Approach to Cybersecurity." BLOG. https://www.fortinet.com/blog/ciso-collective/protecting-your-companys-crown-jewels-from-cybersecurity-attack
98. qtd. in Stefan Palios. (2020, December 03). "Canadian Cybersecurity Leaders Say Ecosystem Requires Community to Grow." Betakit. https://betakit.com/canadian-cybersecurity-leaders-say-ecosystem-requires-community-to-grow/
99. ibid.

Consider two global examples of successful cybersecurity strategy: Israel and Estonia. Less than a decade after Israeli Prime Minister Benjamin Netanyahu declared his vision to shift Israel into "a top-five global cybersecurity power, [. . .] the country has far outstripped its goals: it is recognized worldwide as a cybersecurity innovation hub that continues to produce not only some of the best products and services – but the best minds."[100] While there are obvious differences between Israel, a nation, and Windsor-Essex and Chatham-Kent, a region, there are some important approaches that can be learned from the Israeli model. For one, consider the fact that the Israeli government has "emphasized human capital and not just companies themselves. The process begins at a young age – kindergarten classes involve lessons in computers and robotics. By Grade 4, students are learning computer programming and in Grade 10, they're learning the coding and encryption skills necessary to stop hacking attacks."[101] Of course, elementary and high school education is overseen provincially in Canada, so any type of curriculum change and investment would require broader scale collaboration. However, there remain opportunities for engaging young minds in cybersecurity and training. The oversight and structural limitations should not stop the potential.

As well, Israel invests widely in cyberpreneurship. In 2018, sixty new companies started up. "With assistance from the government," Ferreira writes, "these companies have been allowed to continue to grow to a point where they're attracting the interest of international venture capital funds [which amounted to] $1.04 billion USD across all stages of funding." Israel not only invests in supporting and encouraging cybersecurity as a potential career path, it offers "government-sponsored programs aimed at finding promising youth and providing them with specialized training before and during their military service, [and] the private sector, including non-profits, is also involved in cultivating science and technology education."[102] There are particular advantages that support Israel's progress. Notably, the "talent pool is fed by intelligence units [and] it's exceedingly unusual to come across security startup founders in the country who did not receive their initial training in the intelligence services. This experience also gives these [startup] founders a network of potential co-founders and employees right from the get-go."[103]

The call for mass, broad-scale cybersecurity awareness and training came to Estonia when, in 2007, the country experienced cyberattacks that "crippled the websites of banks, government agencies, and media outlets for weeks."[104] The response in 2008 was a nation-wide strategy that involved citizens and volunteers external to government to protect Estonian cyberspace. The country is now on its third

100. Victor Ferreira. (2019, April 11). "How Israel became a Cybersecurity Power – and What Canada Can Learn from It." Financial Post. https://financialpost.com/investing/how-israel-became-a-cybersecurity-power-and-what-canada-can-learn-from-it
101. ibid.
102. Gil Press. (2017, July 18). "6 Reasons Israel Became a Cybersecurity Powerhouse Leading the $82 Billion Industry." Forbes. https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/?sh=7c6c1856420a
103. Frederic Lardinois. (2020, February 11). "Israel's Maturing Cybersecurity Startup Ecosystem." Tech Crunch. https://techcrunch.com/2020/02/11/israels-maturing-cybersecurity-startup-ecosystem/
104. Monica M. Ruiz. "To Bolster Cybersecurity, the US Should Look to Estonia." Wired. https://www.wired.com/story/opinion-to-bolster-cybersecurity-the-us-should-look-to-estonia/

National Cybersecurity Strategy (2019-22) and "highlights its innovator role at the vanguard of novel cyber approaches."[105]

Certainly, sophisticated attacks and threats require intensive, innovative approaches. Whether mobilizing a region like Windsor-Essex and Chatham-Kent involves enhancing programs and ensuring that average citizens are trained to be cyber aware, or attracting cutting-edge researchers and industry collaborations, the Israeli and Estonian examples reveal that collaboration and collective progress are key.

> "If we want to diversify our economy, it takes time, money, and innovative thinkers – we need a combination of the three to do it right. It doesn't happen overnight."
>
> DREW DILKENS, *Mayor of Windsor*

Mayor Drew Dilkens, in a January 2021 statement about automobility, acknowledges that "if we want to diversify our economy, it takes time, money, and innovative thinkers – we need a combination of the three to do it right. It doesn't happen overnight."[106] It is clear that momentum has been building and there is, perhaps, a sea change coming. From educational programs and industry training opportunities, to high-level funding and government partnerships, the Windsor-Essex and Chatham-Kent region is on a path forward. The need for collaboration, attraction and retention of talent, and a large-scale strategy are part of this region's tech sector narrative.[107] Given the global shifts to remote workforces and the strength of the local research and development efforts, there is an open door for this region to move forward along the cybersecurity path. Incorporating regional strengths such as the historical and current successes with agriculture, automotive, and manufacturing will be important connections to the region's future. If key stakeholders can bridge their interests, if support can be secured from all levels of government, and if the communities in this region are guided towards the open door, there is great promise for this region's cybersecurity future. **Focus will be key.**

---

105. ibid.
106. WEtech Alliance. (2021, January 05). "Welcome to the Automobility Capital of Canada." BLOG. https://www.wetech-alliance.com/2021/01/05/welcome-to-the-automobility-capital-of-canada/#:~:text=%E2%80%9CWindsor%2DEssex%20is%20fast%20becoming,foundation%20of%20manufacturing%20ingenuity%20and
107. Refer to the following two publications for more details: (1) Victoria Abboud and Yvonne Pilon (2020, January 31). Tech Connect: An Initiative to Support the Windsor-Essex Tech Sector. https://www.wetech-alliance.com/2020/02/27/wetech-alliance-releases-tech-connect-report-findings/#:~:text=The%20over%2030%2Dpage%20Tech,recommendations%20based%20on%20the%20research.&text=Tech%20Connect%20lays%20important%20groundwork,community%20and%20elevates%20existing%20opportunities.%E2%80%9D
(2) Julian Villafuerte. (2020, January). Attracting and Retaining Talent in Windsor-Essex: An Essential Guide. Workforce WindsorEssex. https://www.workforcewindsoressex.com/attracting-and-retaining-talent-in-windsor-essex-an-essential-guide/

# RECOMMENDATIONS AND CONCLUDING REMARKS

The future of the Windsor-Essex and Chatham-Kent region depends on the collaborative development of citizens, organizations, companies, and educational opportunities. Based on the research and interviews conducted during this study, it is clear that a successful cybersecurity strategy for this region will require involvement from several areas. Highlighted in Figure 5 (below) are the key recommendations as identified through this report. The recommendations are divided into four specific target areas for ease of reading; however, all recommendations are interconnected and require a linked, intentional approach. The target areas are systems-level levers, research and development, skills and training, and community investment.

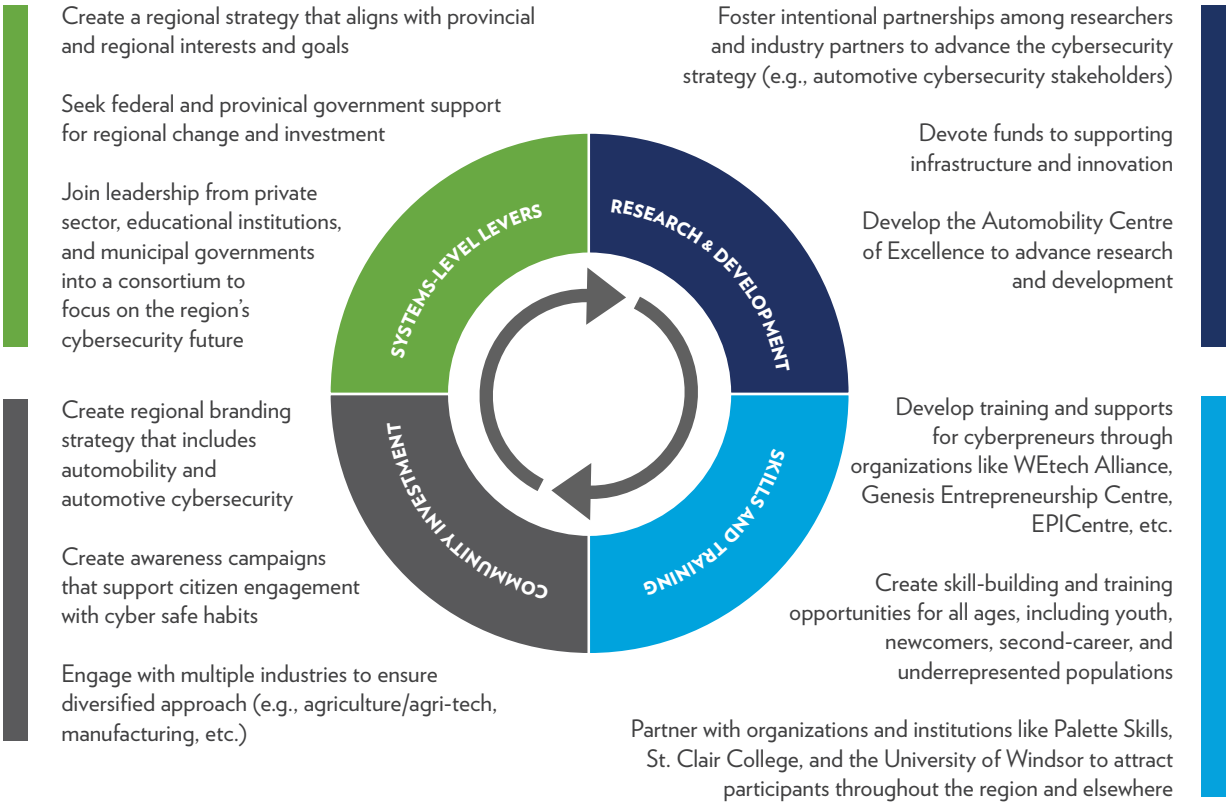



**Figure 5.** Report recommendations divided into four target areas: systems-level levers, research and development, skills and training, and community investment.

The results of this report suggest automobility and automotive cybersecurity as the ways of the region's future. However, given that workplaces are now distributed and remote, there is no limit – no sector or industry limit – to how the region can improve and impact its economic diversity through a focus on cybersecurity. With the numerous sub-domains and influx of researchers, programs, initiatives, and companies, it is clear that this region's progress is limited only by what our perceptions allow.


Cybersecurity is more than an opportunity for jobs. It involves adapting, building, and shaping the future of technology, goods, and even the ways we interact. Our collective abilities to engage, to explore, and to expand our reach rely on our awareness and protection of our cyber interests. The key is ensuring that we move intentionally with clarity of purpose. Focusing on regional collaboration and investment in people and opportunities – in all their diversity – can help us do that.

# RESOURCES


Abboud, Victoria and Yvonn Pilon. (2020, January 31). Tech Connect: An Initiative to Support the Windsor-Essex Tech Sector. https://www.wetech-alliance.com/2020/02/27/wetech-alliance-releases-tech-connect-report-findings/#:~:text=The%20over%2030%2Dpage%20Tech,recommendations%20based%20on%20the%20research.&text=Tech%20Connect%20lays%20important%20groundwork,community%20and%20elevates%20existing%20opportunities.%E2%80%9D

Abbruzzese, Frank. Virtual Interview. 24 November 2020.

---. (2020, 21 October). "How to Keep Your Network Devices Secure." AlphaKOR Academy. AlphaKOR Group. BLOG. https://www.alphakor.com/blogs/it-services/how-to-keep-your-network-devices-secure/

Al-Bernard, Brendon. (2019, February 14). "Canadians Increasingly Looking at Cybersecurity Roles, But It's Still a Job Seeker's Market." Indeed Hiring Lab. BLOG. http://blog.indeed.ca/2019/02/19/cybersecurity-roles-canada/

Bhosale, Amar and Sanyam Agarwal. (2020, October 16). "Cyber Security, Digital Twin, and Trusted Mobility." Telematics Wire. https://www.telematicswire.net/cyber-security-digital-twin-and-trusted-mobility-by-securethings

BlackBerry. (2020, May 11). "The University of Windsor and BlackBerry Partner to Educate Future Data Scientists." Media Release. https://www.blackberry.com/us/en/company/newsroom/press-releases/2020/the-university-of-windsor-and-blackberry-partner-to-educate-future-data-scientists

BlackBerry Cylance. (2020). "2020 Threat Report." https://www.blackberry.com/us/en/products/resource-center/2020-threat-report

Bonnay, Julien. (2020, September 17). "Five Cybersecurity Trends from 2020 – And What the Future Holds." Security: Solutions for Enabling and Assuring Business. https://www.securitymagazine.com/articles/93377-five-cybersecurity-trends-from-2020-and-what-the-future-holds

Campbell, Noah. Email Communication, 20 January 2021.

Canadian Centre for Cyber Security. (2018, December 06). "An Introduction to the Cyber Threat Environment." Government of Canada: Communications Security Establishment. https://cyber.gc.ca/sites/default/files/publications/Intro-to-cyber-threat-environment-e.pdf

Commendatore, Cristina. (2020, May 12). "Trucking Remains a Top Target for Cyberattacks." Fleet Owner. https://www.fleetowner.com/covid-19-coverage/article/21131096/trucking-remains-a-top-target-for-cyberattacks

Coulsey, Brandy. Virtual Interview. 19 November 2020.

Cybersecurity Innovation Centre. 2020. https://www.cybersecurityinnovationcenter.com/

"Cybersecurity Workforce Shortage in Canada." (2019, September 24). BLOG. Whitehorn Merchant Capital. https://www.whitehorncapital.com/whitehorn-blog/2019/9/18/cybersecurity-workforce-shortage-in-canada

Deloitte. (n.d.). "Global Cyber Executive Briefing: Manufacturing." Case Studies. https://www2.deloitte.com/global/en/pages/risk/articles/Manufacturing.html

Deloitte and AVIN. (October 2020). "AVIN Ecosystem Analysis and Roadmap 2020." https://oce-ontario.org/docs/default-source/publications/fy2018-2019-oce-avin-annual-report_final-(2019-06-28).pdf?sfvrsn=2

Deloitte and OCE. (September 2019). "Cybersecurity for Connected and Autonomous Vehicles." https://www.oce-ontario.org/docs/default-source/publications/oce-apma-deloitte_cav-cybersecurity-report_sept-2019.pdf?sfvrsn=2

European Union Agency for Cybersecurity (ENISA). (2019, November). "ENISA Good Practices for Security of Smart Cars." https://www.enisa.europa.eu/publications/smart-cars

"The Epicentre of International Logistics in North America." 2016-2020. WindsorEssex Economic Development Corporation (WEEDC). http://choosewindsoressex.com/transportation. (WEEDC is now known as Invest WindsorEssex).

Ferreira, Victor. (2019, April 11). "How Israel became a Cybersecurity Power – and What Canada Can Learn From It." Financial Post. https://financialpost.com/investing/how-israel-became-a-cybersecurity-power-and-what-canada-can-learn-from-it

Fortinet. (2019, March 08). "Taking a Priority-Based Approach to Cybersecurity." BLOG. https://www.fortinet.com/blog/ciso-collective/protecting-your-companys-crown-jewels-from-cybersecurity-attack

Government of Canada. (2020, September 17). "Statement from the Office of the Chief Information Officer of the Government of Canada on Recent Cyber Attacks." https://www.canada.ca/en/treasury-board-secretariat/news/2020/09/update-from-the-office-of-the-chief-information-officer-of-the-government-canada-on-recent-cyber-attacks.html

---. (2020, August 15). "Statement from the Office of the Chief Information Officer of the Government of Canada on Recent Credential Stuffing Attacks." https://www.canada.ca/en/treasury-board-secretariat/news/2020/08/statement-from-the-office-of-the-chief-information-officer-of-the-government-canada-on-recent-credential-stuffing-attacks.html

Government of Ontario. "Ontario's Skills and Talent Strategy for the Automotive and Mobility Sector." Media Release. Courtesy of Kat Tyrell.

Haldeman, John. Email Communication. 28 January 2021.

Identity Theft Resource Center. (2021, January 28). 2020 in Review: Data Breach Report. https://notified.idtheftcenter.org/s/

Innovation, Science, and Economic Development Canada. (2020, October). Statistical Overview of Canada's Cybersecurity Industry in 2018. https://www.defenceandsecurity.ca/UserFiles/Uploads/publications/reports/files/document-35.pdf

Institute for Border Logistics and Security. (n.d.). "An Overview of Windsor-Essex's Regional Strategy on Automotive Cybersecurity." Unpublished manuscript. Courtesy of Matthew Johnson.

International Data Corporation (IDC) Canada. (2015, December). "2016 Canadian ICT Predictions and Forecast: Digital Transformation and Disruption." qtd. in Public Safety Canada. (2018). National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

International Information System Security Certification Consortium. (2020). (ISC)² Cybersecurity Workforce Study. https://www.isc2.org/Research/Workforce-Study#

Johnson, Matthew. Phone Interview. 16 September 2020.

Jones, Ryon. (2020, October 09). "Waterloo Partnership Launches Cybersecurity Platform in Singapore." Waterloo Stories. https://uwaterloo.ca/stories/waterloo-partnership-launches-cybersecurity-platform?utm_source=ur-newsletter&utm_medium=email&utm_campaign=ur-newsletter

Kadri, Raed. Virtual Interview. 16 November 2020.

Khan, A.J. Virtual Interview. 10 November 2020.

---. (2020, April 29). "ISO21434: Understanding Risks is Key to Ensuring Cybersecurity in CAVs." LinkedIn. https://www.linkedin.com/pulse/iso21434-understanding-risks-key-ensuring-cavs-aj-khan?trk=public_profile_article_view

Kobti, Ziad. Virtual Interview. 07 January 2021.

Lardinois, Frederic. (2020, February 11). "Israel's Maturing Cybersecurity Startup Ecosystem." Tech Crunch. https://techcrunch.com/2020/02/11/israels-maturing-cybersecurity-startup-ecosystem/

Lockhart, Ann. Virtual Interview. 23 November 2020.

MacKinnon, Marc and Galletto, Nick. "Cybersecurity: Everybody's Imperative." Deloitte. https://www2.deloitte.com/ca/en/pages/risk/articles/cyber-security-everybody-imperative.html

Marsh, James. Phone Interview. 21 September 2020.

Mirhassani, Mitra. Virtual Interview. 13 November 2020.

Morrison, Haley. Email Communication. 19 March 2021.

Musson, Jeff. Virtual Interview. 25 August 2020.

National Defence Canada. (2020). The Maple Leaf: Stories about the Canadian Armed Forces and the Defence Team that Supports Them. https://www.canada.ca/en/department-national-defence/maple-leaf.html

Nero, Rea. Virtual Interview. 09 November 2020.

Next Dimension Academy. "Cybersecurity User Awareness Training: Protect Users from Corporate Threats." https://www.nextdimensioninc.com/cybersecurity-user-awareness-training/

North of 41. (2020, Spring). "Top Cyber Challenges Facing Canada: SMB Perspective." Courtesy of Jeff Musson.

Palette Skills. (n.d.) "Accelerated Cybersecurity Training Program." https://paletteskills.org/cybersecurity

Palios, Stefan. (2020, December 03). "Canadian Cybersecurity Leaders Say Ecosystem Requires Community to Grow." Betakit. https://betakit.com/canadian-cybersecurity-leaders-say-ecosystem-requires-community-to-grow/

Press, Gil. (2017, July 18). "6 Reasons Israel Became a Cybersecurity Powerhouse Leading the $82 Billion Industry." Forbes. https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/?sh=7c6c1856420a

Public First. (2020, December). Windsor Works: An Economic Development Strategy for the City's Future Growth. https://www.citywindsor.ca/cityhall/City-Council-Meetings/Meetings-This-Week/Documents/public%20agenda%20February%208,%202021%20special%20meeting%20with%20item%20number%20and%20footer%20with%20appendices%20reduced.pdf

Public Safety Canada. (2018). National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

Rashotte, Rob. (2019, July 04). "The Critical Shortage of Cybersecurity Expertise." Policy Options Politiques. https://policyoptions.irpp.org/fr/magazines/july-2019/the-critical-shortage-of-cybersecurity-expertise/

Research and Markets. (2016, August). "Cyber Security Market – Global Forecast to 2021." qtd. in Public Safety Canada. (2018). National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

Ruiz, Monica M. (2020, February 14). "To Bolster Cybersecurity, the US Should Look to Estonia." Wired. https://www.wired.com/story/opinion-to-bolster-cybersecurity-the-us-should-look-to-estonia/

Saini, Ikjot. Virtual Interview. 02 October 2020.

Sakamoto, Kelsey. (2015). "How Tesla Plans to Lead the Connect Care Experience." Car Throttle. https://www.carthrottle.com/post/how-tesla-plans-to-lead-the-connected-car-experience/

Sartori, Doug. Virtual Interview. 11 January 2021.

Shenfeld, Carly. Email Communication. 04 February 2021.

---. Email Communication. 24 November 2020.

Tesla. (2021). "Software Updates." Tesla Support. https://www.tesla.com/support/software-updates

Tyrell, Kat. Email Communication. 02 March 2021.

---. Virtual Interview. 10 November 2020.

University of Waterloo. (2020, June 03). "Cybersecurity in the Age of COVID." Waterloo Stories. https://uwaterloo.ca/stories/news/cybersecurity-age-covid

University of Windsor. (2020, September 21). "Partnership with Leading U.S. University to Offer Cyber Security Specialty to Odette Grads." Daily News. https://www.uwindsor.ca/dailynews/2020-09-21/partnership-leading-us-university-offer-cyber-security-specialty-odette-grads

Villafuerte, Julian. (2020, January). Attracting and Retaining Talent in Windsor-Essex: An Essential Guide. Workforce WindsorEssex. https://www.workforcewindsoressex.com/attracting-and-retaining-talent-in-windsor-essex-an-essential-guide/

Waddell, Dave. (2021, January 28). "University of Windsor Establishes First Canadian Transportation Cybersecurity Centre." The Windsor Star. https://windsorstar.com/news/local-news/university-of-windsor-establishes-first-canadian-transportation-cybersecurity-centre

--. (2020, September 21). "Windsor Region Gaining Traction in Developing into Auto Cyber Security Hub." The Windsor Star. https://windsorstar.com/news/windsor-region-gaining-traction-in-developing-into-auto-cyber-security-hub

---. (2020, September 17). "Cyber Security Company Moves Headquarters to Windsor." The Windsor Star. https://windsorstar.com/news/cyber-security-company-moves-headquarters-to-windsor

---. (2020, June 29). "Black Boys Code Establishes Windsor Chapter." The Windsor Star. https://windsorstar.com/news/local-news/black-boys-code-establishes-windsor-chapter

---. (2020, May 11). "University Partners with BlackBerry to Create New Cyber Security Programme." The Windsor Star. https://windsorstar.com/news/local-news/university-partners-with-blackberry-to-create-new-cyber-security-programme

WEtech Alliance. (2021, January 05). "Welcome to the Automobility Capital of Canada." BLOG. https://www.wetech-alliance.com/2021/01/05/welcome-to-the-automobility-capital-of-canada/#:~:text=%E2%80%9CWindsor%2DEssex%20is%20fast%20becoming,foundation%20of%20manufacturing%20ingenuity%20and

# ACKNOWLEDGEMENTS

**There are numerous people without whom this report could not have been completed**

With immense gratitude and appreciation for their time and efforts, the author would like to thank: Frank Abbruzzese, Noah Campbell, Adam Castle, Brandy Coulsey, Adam Frye, Mackenzie Habash, John Haldeman, Brian Hendel, Matthew Johnson, Raed Kadri, A.J. Khan, Dr. Ziad Kobti, Ann Lockhart, James Marsh, Dr. Mitra Mirhassani, Haley Morrison, Jeff Musson, Rea Nero, Yvonne Pilon, Dr. Ikjot Saini, Doug Sartori, Carly Shenfeld, John-Marc Vachon, Michelle Teno-Wachter, Kat Tyrell, and the teams at the Autonomous Vehicle Innovation Network, the Institute for Border Logistics and Security, Invest WindsorEssex, the Ontario Centre of Innovation, and WEtech Alliance.

CREATE • INNOVATE • *ACCELERATE*

# WE CAN HELP

WETECH-ALLIANCE.COM

WE·tech ALLIANCE

INVEST WINDSOR ESSEX

investwindsoressex.com