Scaling Cyber

Advancing Canada's Cybersecurity Startups

December 2022

Stephanie Tran and Tiffany Kwok

ROGERS cybersecure catalyst | Catalyst Cyber Accelerator

cybersecure policy exchange
Powered by RBC

Cybersecure Policy Exchange

The Cybersecure Policy Exchange (CPX) is an initiative dedicated to advancing effective and innovative public policy in cybersecurity and digital privacy, powered by RBC through Rogers Cybersecure Catalyst and the Leadership Lab at Toronto Metropolitan University. Our goal is to broaden and deepen the debate and discussion of cybersecurity and digital privacy policy in Canada, and to create and advance innovative policy responses, from idea generation to implementation. This initiative is sponsored by the Royal Bank of Canada; we are committed to publishing independent and objective findings and ensuring transparency by declaring the sponsors of our work.

Rogers Cybersecure Catalyst

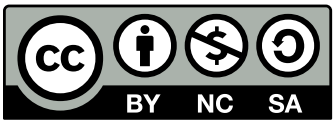
Rogers Cybersecure Catalyst is Toronto Metropolitan University's national centre for innovation and collaboration in cybersecurity. The Catalyst works closely with the private and public sectors and academic institutions to help Canadians and Canadian businesses tackle the challenges and seize the opportunities of cybersecurity. Based in Brampton, the Catalyst delivers training; commercial acceleration programming; support for applied R&D; and public education and policy development, all in cybersecurity.

Leadership Lab

The Leadership Lab is an action-oriented think tank at Toronto Metropolitan University dedicated to developing new leaders and solutions to today's most pressing civic challenges. Through public policy activation and leadership development, the Leadership Lab's mission is to build a new generation of skilled and adaptive leaders committed to a more trustworthy, inclusive society.

How to Cite this Report
Tran, S. & Kwok, T. (2022, December). Scaling Cyber: Advancing Canada's Cybersecurity Startups. Cybersecure Policy Exchange.
https://www.cybersecurepolicy.ca/startups

350 Victoria St, Toronto, ON M5B 2K3



Design
Zaynab Choudhry

Copy-Editing
Cathy McKim

Contributors
Sam Andrey, Director of Policy and Research, Leadership Lab
Karim Bardeesy, Executive Director, Leadership Lab
Sumit Bhatia, Director of Innovation and Policy, Rogers Cybersecure Catalyst
André Côté, Head of Secure and Responsible Tech Policy Microcredential Program, Cybersecure Policy Exchange
Charles Finlay, Executive Director, Rogers Cybersecure Catalyst
Tiffany Kwok, Policy and Research Assistant, Cybersecure Policy Exchange
Stephanie Tran, Policy Analyst, Cybersecure Policy Exchange

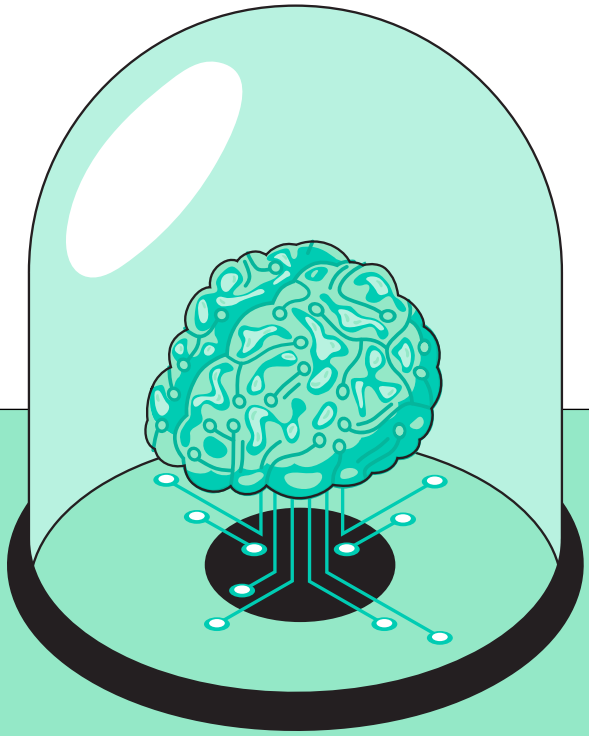
Our work is guided by these core principles:

- Responsible technology governance is a key to Canadians' cybersecurity and digital privacy.
- Complex technology challenges call for original insights and innovative policy solutions.
- Canadians' opinions matter, and must inform every discussion of technology policy.
- Cybersecurity needs to be explained and made relevant to Canadians, and cannot be relegated to language and concepts accessible only to experts.
- Canadian institutions matter, and must evolve to meet new cybersecurity and digital privacy risks to maintain the public trust.
- Harms, inequities and injustices arising from the unequal use or application of technology must be confronted, wherever they exist or could arise.

For more information, visit: https://www.cybersecurepolicy.ca/
@cyberpolicyx @cyberpolicyx Cybersecure Policy Exchange

Executive Summary

The development of new and innovative cybersecurity companies has been recognized by global leaders as critical to advancing both national security and economic growth. For this reason, cyber innovation was identified as one of the three key themes of Canada's National Cyber Security Strategy.[1] Yet, while the country has had some success in creating successful cybersecurity firms, Canada has been struggling to keep up with its geopolitical peers when it comes to successfully bringing new cybersecurity products into the market. Informed by a literature review, jurisdictional scan, interviews and a round-table discussion, this report analyzes the obstacles to commercialization experienced by Canada's cybersecurity startups and the opportunities for overcoming these obstacles.

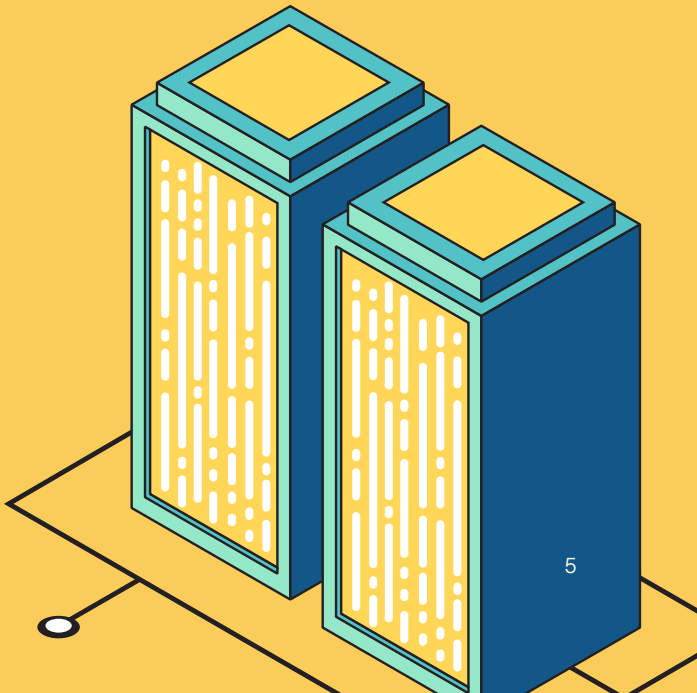


Key commercialization challenges faced by Canadian cyber startups include:

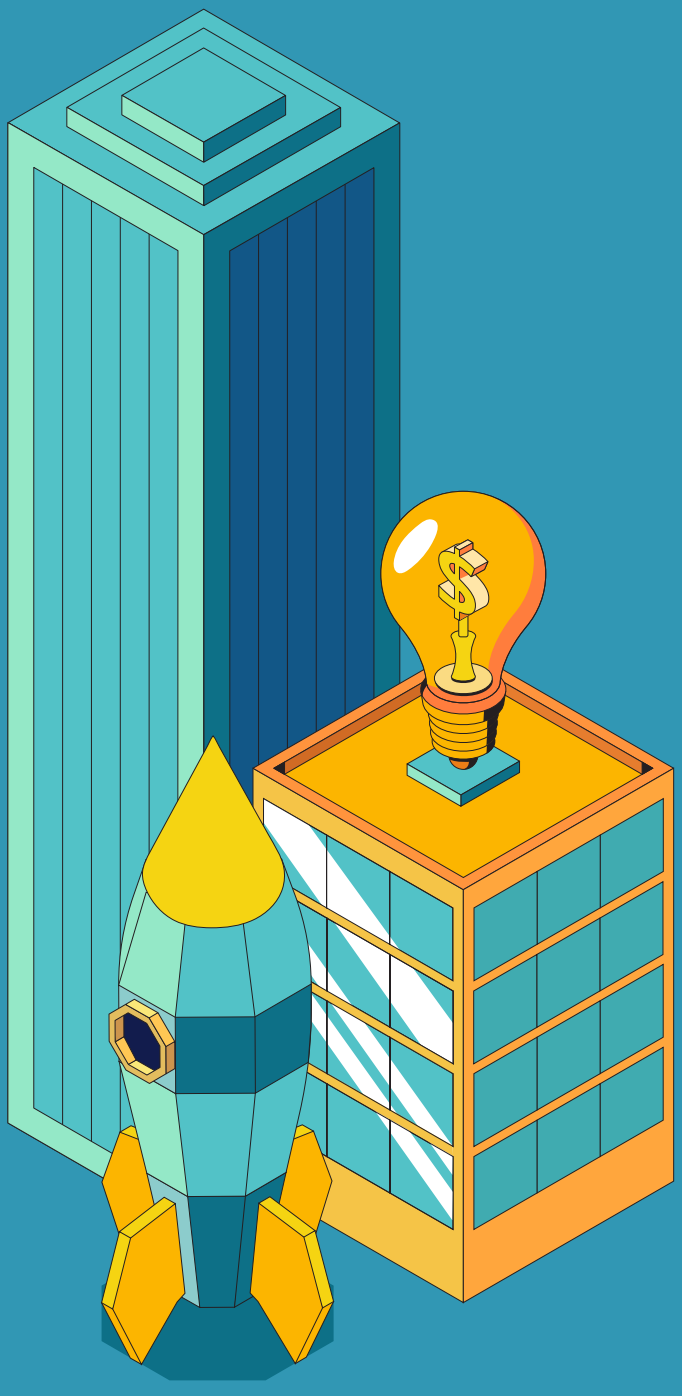
- **A relatively small domestic market:** The limited growth opportunities within the country lead to cybersecurity founders looking for opportunities outside of Canada.
- **Risk-aversion and a lack of innovation mindset in Canada:** Canadian investors and customers are more likely to be risk-averse than their international counterparts.
- **Struggles to secure early adopters:** With insufficient support from the innovation ecosystem to help startups find initial customers, entrepreneurs typically rely upon existing connections or personal referrals to find their first customers.
- **Procurement hurdles:** Canadian public procurement processes are often too time-consuming and arduous for smaller businesses, limiting opportunities for governments to act as early purchasers and validators.
- **Lack of cybersecurity expertise and connections among investors:** Canadian startups feel that investors are less familiar with cybersecurity than other digital technology subsectors, leading to challenges in securing funding for continued growth of their product.
- **Lack of perceived value of IP protection:** Canadian cyber startups struggle to find support for IP protection, and also struggle to see its utility when confronted with the high costs and time requirements for patent filing.

Canada's startup community comprises many players who can help step foster a more sustainable cyber innovation ecosystem. This includes academic institutions, governments at all levels, investors, industry, incubators and accelerators, non-profit intermediaries, and startups themselves. The development of a more coherent, connected, focused and goal-aligned cyber ecosystem will be important for addressing Canada's cybersecurity challenges and creating the conditions for the growth of successful new cyber companies. Key areas of opportunity include:

1. **Connecting startups to early adopters:** Successfully connecting entrepreneurs to initial customers is vital to their success. Facilitating product development and validation, and piloting government procurement approaches that provide advantages for Canadian businesses, could help close the gap in securing early adopters.
2. **Lowering IP protection costs:** Introducing more funding to compensate the costs of IP protection efforts can help incentivize entrepreneurs to pursue IP ownership.
3. **Closing the risk-aversion gap:** Initiatives to build cybersecurity knowledge among investors and improving data sharing among ecosystem members can help reduce risk aversion among investors. Targeted public investment can be introduced to ensure support for promising startups when investors decline ventures.
4. **Encouraging diversity:** Improving the inclusion of under-represented demographics among cybersecurity talent and within the investment sector can advance the equity of investment decisions and strengthen innovation efforts.



Introduction



01

Introduction

The need for a focused approach to grow and support a dynamic national cyber innovation ecosystem in Canada is more urgent than ever. In the 21st century, cybersecurity has emerged as an imperative for national security and nation state competition. As with many technological innovations in history, economic and geopolitical power are at stake in this competition for technological dominance.[2] Global technology leadership in the cybersecurity domain has the potential to enhance a country's global power and security, whereas failure to build national cyber capacity will pose a threat.[3]

There is also an economic imperative for Canada. Successful commercialization of cybersecurity innovations allows the country to benefit from economic and social gains realized through increased jobs, increased economic activity, and more. Canada's success has been mixed. Approximately 350 cybersecurity companies have their headquarters in Canada.[4] According to Crunchbase, Canada ranked fifth globally in cybersecurity venture capital (VC) funding in 2021 — ahead of several larger economies, including Japan, Germany, France and India.[5] Yet, despite this public and private investment in Canadian cybersecurity firms, experts continue to emphasize the country's struggle to commercialize research innovations, and to grow and scale new companies into national and global champions. Unable to secure investment and find customers in Canada, cybersecurity entrepreneurs are often moving their operations and intellectual property (IP) outside of the country. As one person stated to the Ontario Expert Panel on Intellectual Property, "Canada is the world's open source factory for ideas. We create it, but let others commercialize it."[6]

Evidence from Canada and international peers suggests that building a dynamic and sustainable cybersecurity innovation ecosystem in Canada will be vital to addressing the country's domestic cybersecurity threats, supporting entrepreneurs to grow successful cyber companies, and positioning the country as a leading cyber actor in the global digital economy. Yet, today, the Canadian cyber innovation ecosystem remains underdeveloped and fragmented, lagging behind those in peer countries like the United Kingdom and the United States. These are limiting opportunities for growth among a burgeoning community of Canadian cyber startups, whose successes are key in meeting both national security and economic goals.

Why is that and what can be done? This paper seeks to examine this question by assessing the state of cybersecurity innovation in Canada; exploring cyber innovation approaches and models in other jurisdictions; and identifying an actionable set of opportunities to be taken by players within Canada's cyber innovation ecosystem to accelerate commercialization.

Methodology

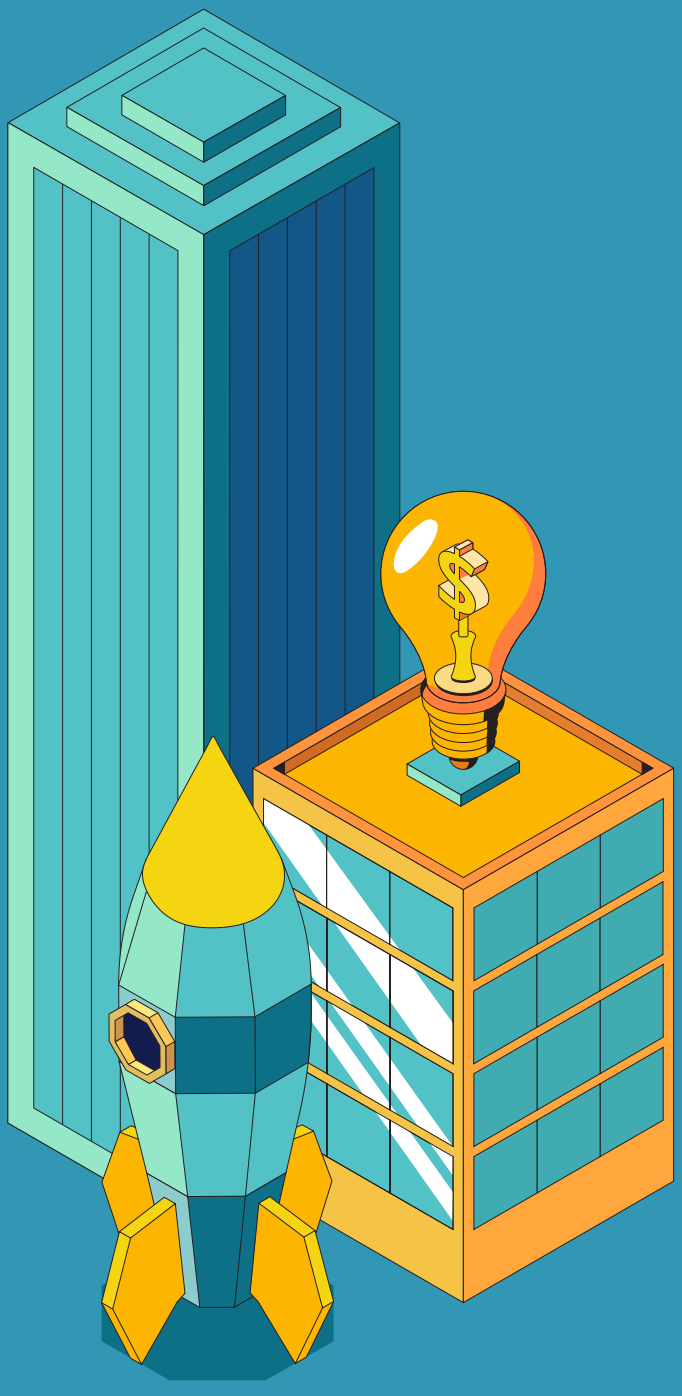
The focus of this report is exploring how to build a dynamic and sustainable cyber startup ecosystem in Canada that drives both innovation and commercialization. The research that informs our findings is derived from:

- A **literature review** of the current state of commercialization in the cybersecurity startup ecosystem, the Canadian cyber startup marketplace, the procurement landscape, and understanding cyber-specific challenges/issues;
- A **jurisdictional scan** to identify notable approaches and frameworks being used in other global regions that can be adopted in the cyber ecosystem; and
- **Interviews** and a **roundtable discussion** with Canadian cyber startups, government, and entrepreneurship ecosystem representatives, to understand current circumstances, challenges and opportunities for growing cyber startups in Canada.

The roundtable was conducted under the Chatham House Rule. The names of interviewees and roundtable attendees are disclosed in the Appendix with the participants' consent.

Throughout this report, the term **"cyber startup"** will be used to describe companies specializing in cybersecurity that have their roots as startups and that are going through the startup journey. This can encompass early-stage startups, scale-ups and unicorns;[7] ultimately, our use of the term focuses on entrepreneur-led cybersecurity companies. Although we recognize that contexts and technologies can greatly differ between cybersecurity companies, for the purposes of our paper, we apply a broad interpretation of cybersecurity companies as those that offer products and services related to information and network security.

Canada's Cyber Innovation Ecosystem



02

Canada's cyber innovation ecosystem

Canada's cyber innovation ecosystem is composed of various stakeholders, which include startups, academic institutions, governments, investors (both domestic and international), incubators and accelerators, industry and non-profit organizations. Each group of actors plays an important and distinct role within the ecosystem, with Canadian and international evidence suggesting that the alignment of goals and coordination of activities is key to collective success. As the expression goes, the whole is greater than the sum of the parts.

Startups

Startup founders generally consist of entrepreneurs that are developing a cybersecurity product or service, and are working to commercialize it both domestically and globally. They are a key driving force for innovation in the ecosystem, as their ideas and expertise fill gaps in the cybersecurity needs of the country. Startup founders generally also collaborate with, receive and engage with support provided by other stakeholders in the ecosystem. Canadian examples include Flare Systems and Arctic Wolf, two startups that have found tremendous success. Flare Systems was founded in 2017, by Mathieu Lavoie, Israël Hallé and Yohan Trépanier Montpetit, focusing on scanning the digital footprints of organizations. Since its inception, the startup has experienced tremendous growth in Canadian markets, raising $9.5M CAD in series A funding in June 2022, been a part of the Rogers Cybersecure Catalyst, and is currently considering expansion into U.S. markets.[8] As for Arctic Wolf, co-founders Kim Tremblay and Brian NeSmith founded the company in 2012, focused on providing security monitoring to detect and respond to cyber threats. Arctic Wolf has likewise undergone successful growth, running its headquarters in Minnesota and performing R&D operations in Waterloo, Ontario, the company has recently been named to the Forbes 2022 Cloud 100 in August 2022.[9]

Academic Institutions

Academic institutions play another major role in the Canadian cybersecurity ecosystem, as Canada's multitude of world-class universities and colleges develop homegrown talent and produce innovative research.[10] Amidst continual global high demand for tech talent and ongoing insufficient supply, Vancouver and Toronto had the largest tech talent workforce gains in 2021 compared to the rest of North America.[11] In addition to contributing to the talent pool and development of IP, faculty and researchers within these institutions also create startups to commercialize their work. Canada's post-secondary schools are also working to facilitate the management and commercialization of IP developed in their institutions. Several universities have created their own IP commercialization offices in order to encourage the commercialization of their research innovations.[12] In an effort to reinforce this work, the Ontario government's Commercialization Mandate Policy Framework required all publicly-assisted Ontario post-secondary schools to

develop IP commercialization policies for their institutions.[13]

Governments at All Levels

Federal, provincial/territorial and municipal governments across Canada play a key role in the ecosystem through their offerings of various programs, tax incentives and grants to encourage innovation, investing in products and services, and guiding the country's innovative path through policy.[14] Government contributions include economic development programs, tax incentives, policy guidance and awareness development.

Economic development programs

One way that the government contributes to the ecosystem is through initiatives aimed at advancing the research, development and adoption of cybersecurity innovations. The federal government's Innovation for Defence Excellence and Security (IDEaS) program is an example of this engagement through supporting early-stage startups with opportunities for funding, product testing and pilot projects with departments within the Department of National Defence (DND) and the Canadian Armed Forces (CAF).[15]

Procurements

The federal government's Industrial and Technological Benefits (ITB) policy requires defence procurements over $100 million that are not subject to trade agreements, or for which national security exceptions are invoked, to undertake business activity in Canada equal to the value of the contract. This can include building the product or providing the service in Canada; or through R&D, skills development, or purchasing goods and services from Canadian suppliers; and often requires a minimum proportion be spent on small- and medium-sized businesses, and on a list of Key Industrial Capabilities (KICs), which since 2018 has included cybersecurity.[16]

Policies

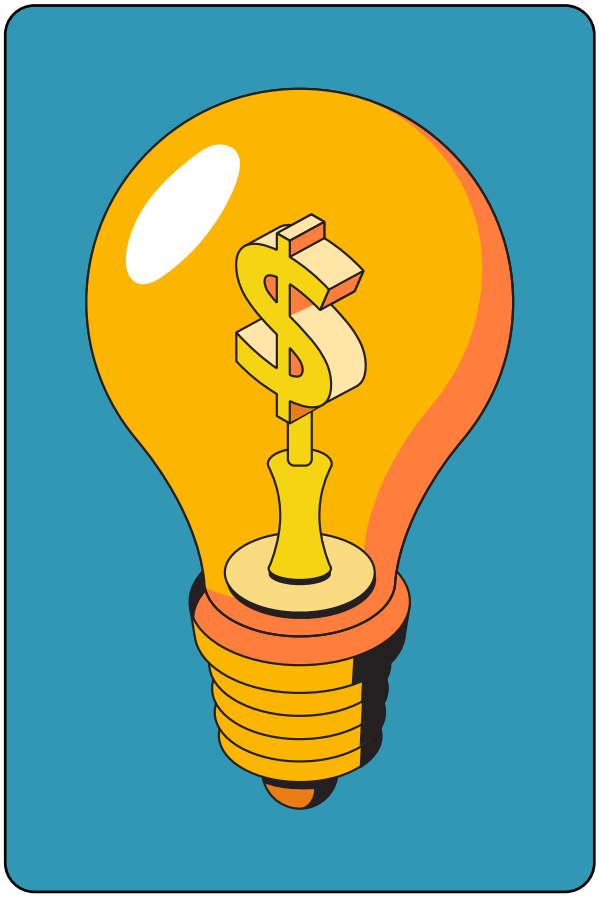
Government policies also shape the cyber ecosystem by regulating activities and putting forth cybersecurity policy objectives. A federal example is the National Cyber Security Strategy, which describes Canada's agenda for advancing cybersecurity and cyber innovations. Fostering cyber innovation is one of the three key themes outlined in the strategy. It affirms that the government plays a role in supporting the growth of innovative cyber startups "to bring cyber security technologies and services to the global marketplace."[17] The Strategy states that the Canadian government will take actions to stimulate investment, and research and development of cyber innovations.

Information sharing

Information sharing from government entities also impacts the ecosystem through building collective understanding of the cybersecurity landscape, and by building awareness of the significance of cybersecurity. Government bodies such as the Canadian Centre for Cyber Security (Cyber Centre) and Ontario's Cyber Security Centre of Excellence provide cybersecurity guidance and information that help key stakeholder groups such as investors recognize the importance of cybersecurity.

Investors

Investors, both domestic and international, are another stakeholder within the ecosystem, including but not limited to venture capitalists (VCs), angel investors, chartered banks, corporates, foreign multinational enterprises, and institutional investors such as pension funds. These bodies provide financial capital to startups, to support business growth from early-stage product and service development and commercialization, to later stage growth and expansion.[18] The backing behind Canadian startup SecureKey reflects the diversity of investor groups, having received funds from Canadian banks and companies, including Desjardins Group, Rogers Communications Inc. and BCE Inc.[19]



Industry

Industry members consist of private sector organizations, spanning from small- and medium-sized enterprises to large corporations. Companies can act as purchasers of products and services from cyber startups, and can also contribute expertise to industry initiatives and public policy consultations.

Incubators and Accelerators

Incubators and accelerators play a vital role in connecting aspiring and existing startups to other parts of the ecosystem, and providing startup skills and resources for founders. Incubators help startups in their very early stages build their ideas and develop their business models.[20] Accelerators are more selective, with the aim to rapidly grow promising startups, including the added benefit of providing seed funding for these firms.[21]

Incubators and accelerators can differ in business models, market sector focus and scope. Canada's big non-profit players include MaRS, Communitech and NEXT Canada. For-profit innovation firms include DMZ Ventures and Highline Beta. Some groups are also focused on a region or locality, such as InvestOttawa and the New Brunswick Innovation Foundation. Moreover, some incubators and accelerators focus on specific sectors, with the Rogers Cybersecure Catalyst being the only accelerator with a sole focus on cybersecurity.

Non-Profit Intermediaries

Professional associations such as the Canadian Council of Innovators provide representation and resources for cybersecurity startups, helping to bridge the gap between startups and industry. Contributions by these organizations include providing access and advice on hiring talent, getting access to capital, and finding customers. The Canadian Cyber Threat Exchange (CCTX) is another group that brings together Canada's private sector members, with a larger focus on cyber threat information sharing.[22]

Standards bodies also play a role by developing guiding principles for the cybersecurity industry. One example is the CIO Strategy Council, which develops voluntary standards for tech innovations in areas, including artificial intelligence, biometrics and cybersecurity.[23]

The Cyber Innovation Ecosystem

What makes cybersecurity startups different?

Through the research activities, and interviews and discussions with leaders and experts from Canada's cybersecurity ecosystem, a foundational question was explored: are the conditions for cyber startup firms different than for startups in other digital technology sectors and, if so, how?

Three key distinctions were highlighted: (1) clearer return on investment (ROI) horizons in other startup industries; (2) the heightened need for cyber startups to build trust with prospective customers in order to secure early adopters; and (3) cybersecurity being a business enabler across industries, with the potential for a larger pool of buyers.

Less obvious ROI indicators compared to other industries

Many interviewees shared that cybersecurity differs from other innovation markets due to the increased difficulty of demonstrating an ROI in cybersecurity products and services compared to other markets. Investors have been noted to see obvious benefits out of other technologies such as clean tech, biotech and fintech products, whereas cybersecurity products require a longer-term investment perspective to recognize business benefits. Interviewees also noted the need to demonstrate cybersecurity ROI in different ways, as the realized benefits may look different, with examples including reducing threats and IT support costs.

Higher trust threshold for early adopters

Interviewees repeatedly highlighted the need to build trust – and the challenge of building trust – with clients, particularly due to the mission critical nature of cybersecurity. Successful cybersecurity startups have been generally reliant on existing trusted networks, or have invested heavily in building trust with early adopters.

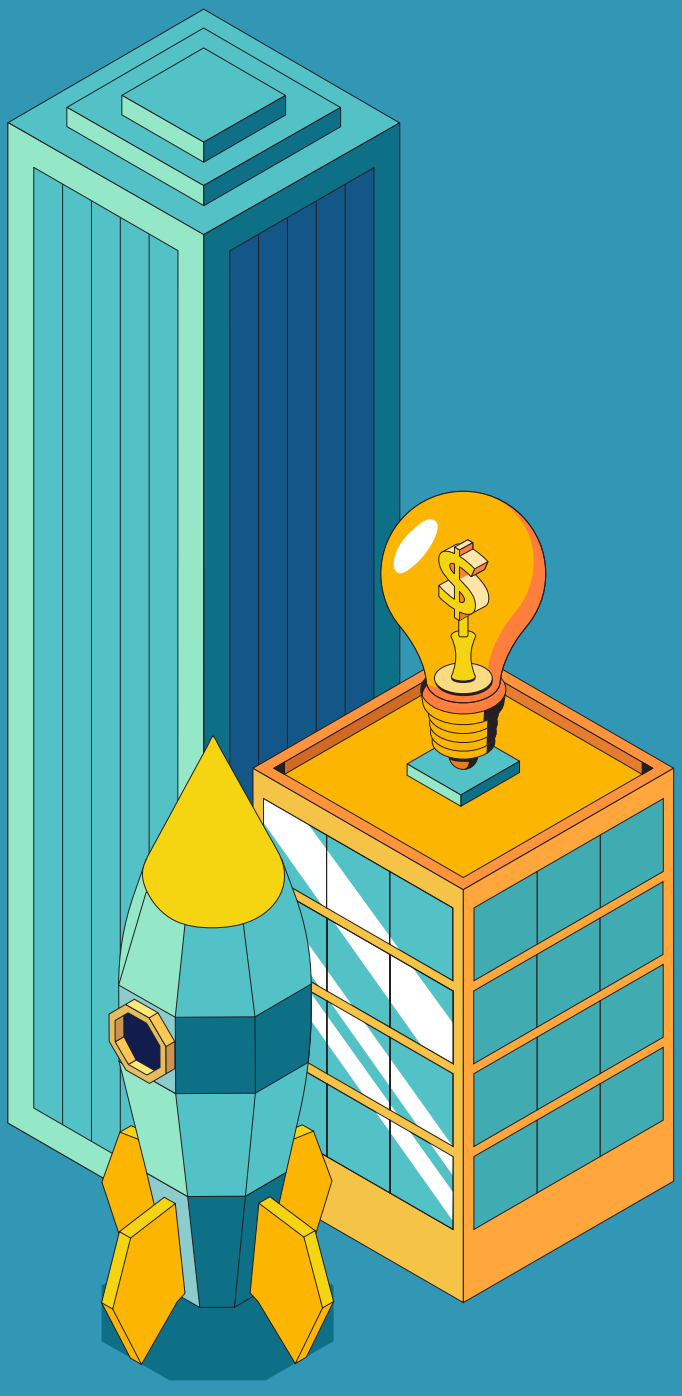
A business enabler across industries

Another frequently noted difference between cybersecurity and other markets is the fact that cybersecurity is required across all industries and organizations. The ubiquity of computer systems, data and data protection means cybersecurity products and services are not limited to a small pool of potential buyers. Despite this, interviewees noted the difficulty in getting investors and company executives to understand the necessity of cybersecurity in their operations, suggesting this due to a lack of understanding surrounding threats, or a fear of not knowing how to deal with cybersecurity-related matters.

"Battle for the same dollar"

However, interviewees also stressed the commonalities among all startups, such as the need to find product market fit and secure sales, as well as facing the same obstacles to breaking into the market regardless of industry. Others mentioned the "battle for the same dollar", with the view that startups across all markets are competing for VC investment and government program funding.

The Cybersecurity Market

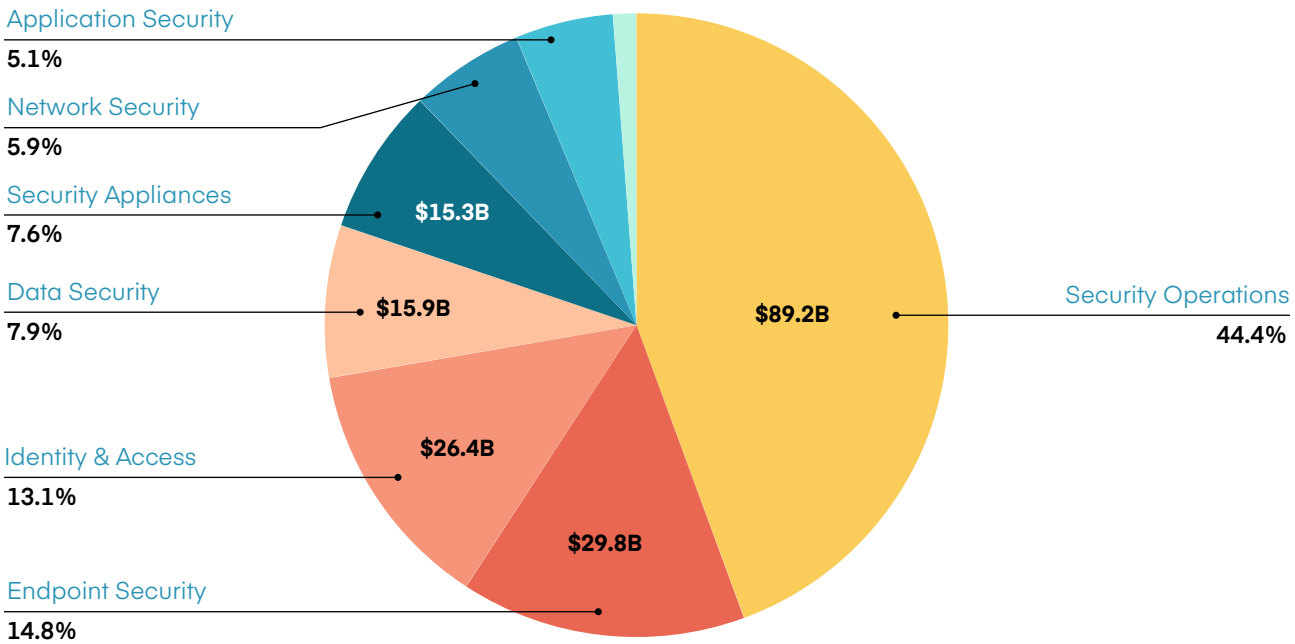


03

The Cybersecurity Market

The global cybersecurity market is estimated to be approximately $170 billion USD.[24] Last year saw significant investments into cybersecurity ventures, with over $21 billion USD raised globally, compared to just approximately $9 billion USD the year before.[25] This market segment is rife with opportunities for startups both in terms of demand and early funding, as the cybersecurity industry has more early-stage investment activity compared to other industries globally.[26] The high volume of early-stage deals for cybersecurity ventures continued during the first half of 2022 despite the decline in overall cybersecurity investments compared to 2021.[27] The drop in overall cybersecurity venture funding is a reflection of the current slowdown in tech investments generally amidst a market downturn.[28] Products and services by cybersecurity startups are also highly sought after by Chief Information Security Officers (CISOs) seeking distinct cybersecurity offerings.[29]

Global Cybersecurity Market Size Estimate ($USD B)



Source: Pitchbook (2022)

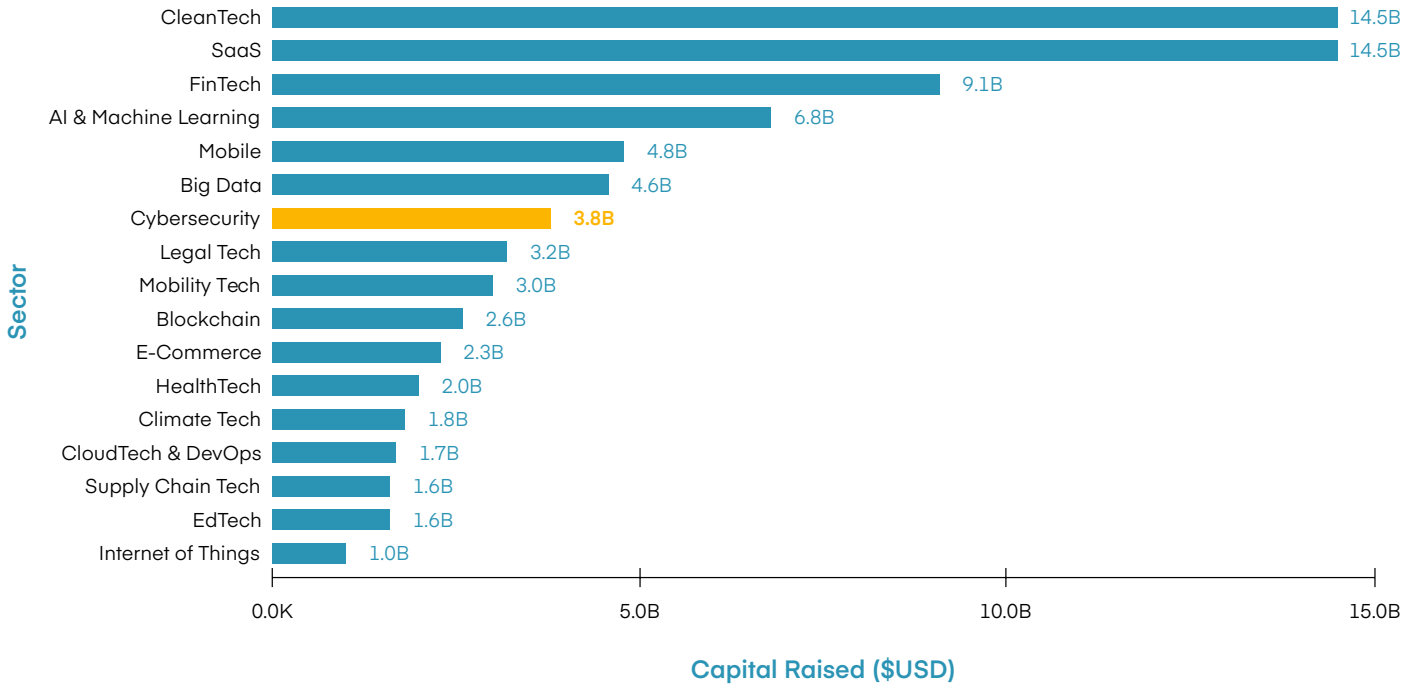
Canada's cybersecurity market

The massive size of the cybersecurity market is reflected in its major presence in Canada. According to Pitchbook, there's over 350 Canadian cybersecurity companies whose headquarters are located in the country. Almost 60% of those companies are based in Ontario, with the City of Toronto holding the highest number of cyber firms (76 companies, encompassing 22% of Canada's cyber industry). British Columbia and Québec rank 2nd and 3rd in terms of number of cybersecurity companies with 18% and 13% of cyber firms, respectively. Despite being the home of up-and-coming companies such as TrojAI and Beauceron Security, New Brunswick holds only 1% of Canada's cybersecurity companies, along with Newfoundland and Labrador, Saskatchewan and Manitoba.

In 2021, Canada's cybersecurity companies raised around $3.8 billion USD in capital.[30] Other tech sectors such as clean technology, financial technology and AI exceeded this amount, with FinTech raising over twice as much capital compared to cybersecurity.[31] In terms of revenue, Canada's cybersecurity industry is expected to generate $3.5 billion USD in 2022, while the U.S. cyber market is forecasted to produce over $64.8 billion in revenue this year.[32]

Capital Raised for Canadian Tech Verticals in 2021

Source: Pitchbook (2022)



Note: Companies can be classified in multiple verticals so these figures are non-cumulative.

HQ Province	Location	Companies	% of Canadian Companies
Ontario		**203**	**58%**
	Toronto	76	22%
	Ottawa-Nepean	46	14%
	905 Region	44	13%
	Kitchener-Waterloo	20	6%
British Columbia		**64**	**18%**
	Vancouver	39	11%
	Victoria	8	2%
Québec		**48**	**13%**
	Montreal	30	9%
	Québec City	4	1%
Alberta		**17**	**5%**
	Calgary	11	3%
	Edmonton	4	1%
Nova Scotia		**8**	**2%**
	Halifax	5	1%
New Brunswick		**5**	**1%**
Newfoundland and Labrador		**3**	**1%**
Saskatchewan		**2**	**1%**
Manitoba		**2**	**1%**

Cities with less than 4 companies have been omitted. Source: Pitchbook (2022).

Global cyber industry leaders

Within the global cybersecurity market, there are several countries that have charted above Canada in terms of cybersecurity investment and sales. The international scan zoomed in on three of the peer countries behind which Canada lags, and the lessons they offer for Canadian cyber ecosystem development: the United States, Israel and United Kingdom.

United States

Consistently ranking 1st in the world for cybersecurity investment since 2011, the U.S. cybersecurity market's revenue is projected to reach $65 billion USD in 2022.[33] Many interviewees noted the U.S.'s abundance of innovative R&D programs, higher density of opportunities for investment, and government-led initiatives leading cybersecurity research. Examples of innovative R&D programs mentioned include the Defense Advanced Research Projects Agency (DARPA), the Intelligence Advanced Research Projects Agency (IARPA), the Small Business Innovation Research (SBIR) program and the VC program In-Q-Tel. All of these programs are either funded by, or include heavy government involvement, and operate within the realms of defense, intelligence and small business innovation research.[34] For In-Q-Tel, startups that are chosen are given ample financial resources, market understanding, engineering expertise, and connections to government partners and portfolio companies.[35] This supports the long-term growth and financing of selected startups, based on market or government needs.[36]

Government-led support has also been a vital aspect in directing and supporting cyber startups and innovation, through different initiatives such as U.S. Federal Government Initiatives on Cybersecurity Research (2009-2011), Department of Homeland Security Cybersecurity Research Programs, and a cybersecurity council established within the U.S. Chamber of Commerce. The combination of innovative R&D programs, an abundance of investment opportunities, and a government-led drive to cyber innovation have positioned the country as a global leader in the cybersecurity industry. As for investment opportunities, many interviewees found that the larger presence of angel investors, VCs and an overall less risk-averse attitude has provided greater funding opportunities in the U.S. for cybersecurity startups. Comparing the U.S. venture capital scene to the Canadian one, David Shipley, Co-founder and CEO of Beauceron Security, described the apprehensive nature of Canadian investors, whereas U.S. VCs are more willing to take a chance.[37]

Israel

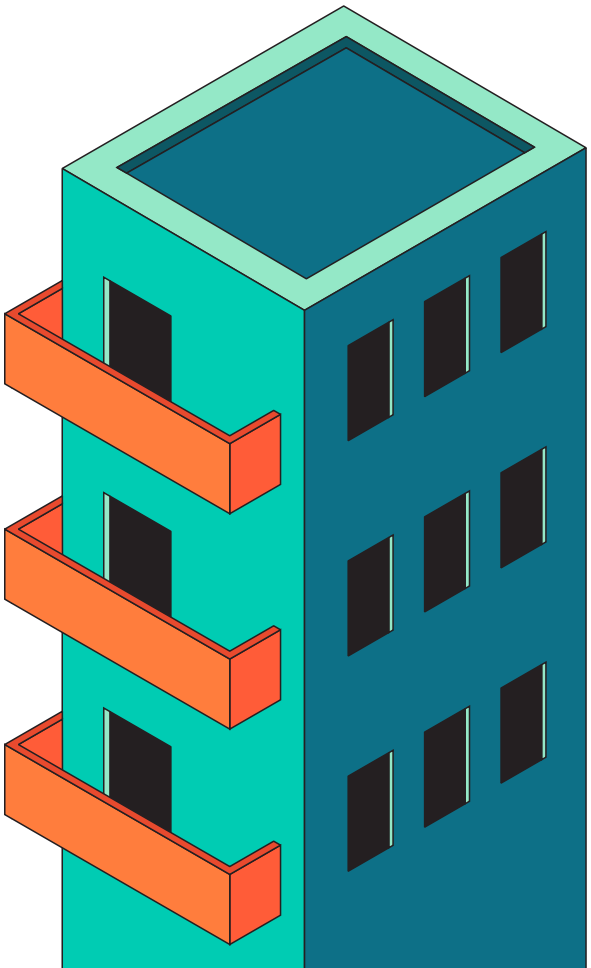
Israel currently ranks 2nd for global cybersecurity investment after the U.S., with massive jumps in the number of active cybersecurity companies, and funding amassed to $8.8 billion USD in 2021.[38] Multiple interviewees attributed much of the country's strength to strong government-backed innovation initiatives and the streamlining of former military personnel into the cybersecurity industry. Government-backed innovation bodies and initiatives include Israel Innovation Authority, involvement from the Israel National Cyber Bureau, and the National Cyber Security Authority. Israel's approach consists of a significant focus on R&D, with efforts to connect military research, intelligence activities and the

private sector. Due to its compulsory military service for 18- to 21-year-olds, Israel has an abundance of trained security personnel whose skills are transferable to cybersecurity work.

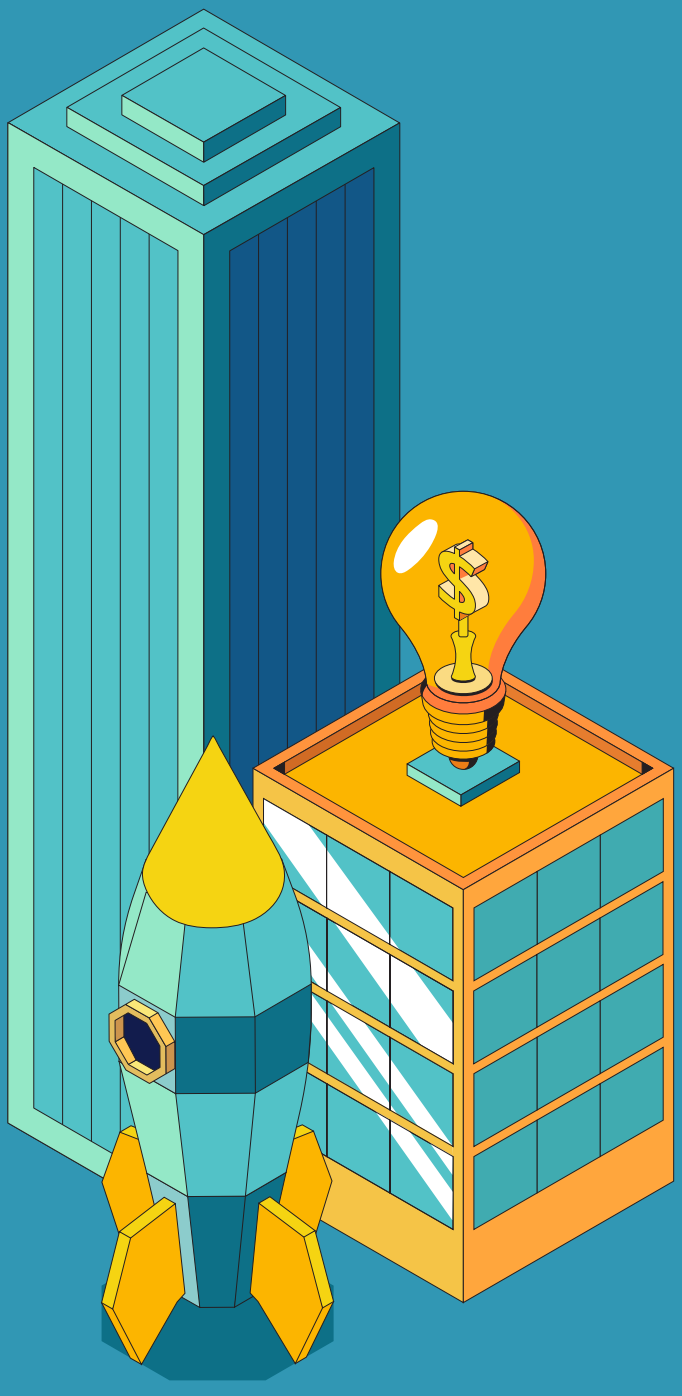
With the close link between their cybersecurity R&D and national security endeavours, Israel's cybersecurity innovation model can be seen as driven by their distinct geopolitical context. These distinct conditions make the adoption of Israel's precise cybersecurity innovation model less realistic for Canada. Interviewees noted the unlikelihood and uncertainty of Canada being able to adopt a similar framework, stating that Canada will have to find and adopt a model that works for the country's needs, demographics and circumstances.

United Kingdom

The United Kingdom has been another global leader in cybersecurity investment, placing 4th in the world in 2011-2020, with its cybersecurity market's revenue projected to reach approximately $10 billion USD in 2022.[39] The country's success has been attributed to the ease of access to larger, international markets, accelerators, high rates of public procurement and government-funded programs.[40] The UK government has established a multitude of programs and initiatives for startups. For instance, the Cyber Runway Scale Programme has helped tech startups commercialize through facilitating contracts between companies and new public and private sector customers.[41] Government support for cybersecurity startups has also been evident in their procurement practices, with British cybersecurity companies viewing public procurement as having been helpful in their efforts to scale.[42] Apart from the programs themselves, several interviewees also noted the difference in greater government involvement in leading cybersecurity innovation, providing as an example the UK's GCHQ (Government Communications Headquarters), which is involved in defence of communications, while also actively working to advance cyber economic opportunities in the country.



Canadian Commercialization Challenges



04

Canadian Commercialization Challenges

Commercialization of research and IP has been a longstanding challenge in Canada. Over the years, Canadian policymakers, academics and industry members have worked to examine the causes and implications of Canadian innovators developing their ideas in Canada, but ultimately moving their companies and/or IP outside of the country. Gallini and Hollis (2019) describe this as a paradox, whereby Canada's internationally competitive capacity to produce inventions is met with lackluster levels of innovation outputs.[43] IP lawyer James Hinton emphasized the implications of this paradox in his presentation to the House of Commons Standing Committee on Industry, Science and Technology in 2017, stating that "Canadians are doing the hard work to create great technologies, but we are not able to benefit from them. This further prevents us from being able to reinvest in new technologies and new industries."[44]

These challenges appear to be present in Canada's cyber startup ecosystem as well. Many interviewees felt that cybersecurity startups were not incentivized to operate and grow in Canada. Although entrepreneurs are finding success in inventing and building their products in Canada, their progress falters as they struggle to commercialize and scale within the country. Our research identified several key obstacles to cybersecurity startup growth, including Canada's relatively small domestic market, lack of early adopters, dearth of cybersecurity expertise among investors, and lack of diversity of investors.

Relatively small domestic market

One of the major obstacles to growth faced by Canada's cybersecurity startups is the relatively small size of the domestic market in comparison to the U.S. or EU. The limited opportunities for growth within Canada alone have cybersecurity founders focus on scaling business outside of the country.

It has long been recognized that, in Canada's domestic market, there is "insufficient demand to sustain firms and industries in leading edge technologies or products."[45] This relative lack of domestic demand drives startups to "seek capital abroad, move their sales or business abroad, or sell."[46] Interviewed startup founders shared similar sentiments about the larger opportunities for growth outside of Canada, with some feeling that the only way to find success as a startup was to move outside of Canada, rather than try to scale through exports from Canada. One founder felt grateful for having international contacts prior to founding their startup, feeling that an absence of these international connections would have prevented their company from finding success.[47]

Several interviewees shared intentions to move their offices to "where the customers and opportunities are." These founders have set plans to move to the U.S. and the EU in order to access more funding opportunities, larger client bases, and cybersecurity talent. Ian Paterson, CEO of Plurilock, described Canada's dearth of

resources necessary for cybersecurity startups: "Resources are not here. Talent is not here. Financial incentives are not here. Network is not here. Capital is not here. We have a base of application developers, but not cybersecurity folks. We have good funding and talent in software engineers but not in cybersecurity."[48]

Research has shown that Canadian businesses seek a merger or acquisition by foreign firms at a higher frequency than European companies.[49] A recent paper published by the ICTC describes how Canadian VCs may be placing more pressure on startups for earlier acquisition compared to American VCs since "Canadian companies take longer to obtain their first round of financing, go through fewer rounds of financing overall, and raise less money before exiting."[50] Under these conditions, Canadian founders are incentivized to sell their startups early rather than continue their struggles to scale. As one founder put it, "it's hard to fault an entrepreneur for cashing out given how difficult it is out there. If the deal is on the table, they will likely say yes to the deal."[51] However, some economic activity can still be realized in Canada after founders sell their startups abroad. Founders can reinvest their newly-found capital into new startups, building new innovations in their home country.[52] The operations of the acquired company may also still remain in Canada despite its assets being owned by a foreign firm.

A risk-averse mindset

A common theme that emerged, underlining many of the hurdles to commercialization faced by cybersecurity startups, is lack of an innovation mindset in Canada. Canadian investors and customers are more likely to be risk-averse than their American counterparts, and thus tend to be less willing to invest or purchase from early Canadian startups.

Canada's risk-aversion and its implications for innovation is well-documented in the literature. A 2019 study found that Canada's risk-aversion was reportedly a "significant challenge" for entrepreneurs conducting business in the country.[53] In a 2015 report, the Business Development Bank of Canada (BDC) explained how the lower risk tolerance of Canadian businesses compared to American ones may be partly due to our "smaller domestic market, more risk-averse financial institutions or cultural differences".[54] This aversion to risk leads to underinvestment in Canada's startups, leaving entrepreneurs struggling to commercialize their products and scale.

The Canadian government has been advised to address the country's lack of innovative mindset in the past, with the Advisory Council on Economic Growth receiving a significant amount of feedback in 2017 urging for the development of an improved 'innovation culture' in Canada with "higher tolerance for risk and failure."[55] Despite these previous calls, Canadian cybersecurity entrepreneurs are still struggling to commercialize, with investors and potential buyers remaining too cautious to provide support for early cybersecurity ventures.

Hesitant buyers

The hesitance of Canadian buyers and investors in being early adopters or providing startup funding has forced a majority of interviewed founders to seek growth elsewhere. Grant Colhoun, Founder and CEO of Okanii, found American clients to be much quicker at

decision-making than those in Canada.[56] The slowness and lack of actualized deals has led Colhoun to turn to the U.S. for business. TrojAI's Co-Founders James Stewart and Stephen Goddard were also enticed to shift their focus outside of Canada after struggling to attract early adopters within the country.[57] Plurilock CEO Ian Paterson also found it easier to get early purchases from the U.S. compared to in Canada. Paterson described the difficulty of selling domestically, stating how, "on the commercial side, there's a hesitancy from large corporations. It's impossible to land a Canadian bank as a first customer. Even today after selling to different financial institutions, it's still difficult to land a Canadian bank."[58] This reluctance on the part of Canadian buyers to be early customers leaves startups, desperate to secure initial sales, to focus their attention outside of Canada.

More cautious investors

Cybersecurity founders also found Canadian investors to be much less willing to accept risk than foreign investors, which results in smaller investments and slower processes. CybernetIQ's Founder Joe Cummins felt a disconnect between Canadian investors and the reality of early startup development: "Canadian shareholders want to put in lower amounts expecting a higher upside. The inverse is true in the U.S. where they have massive cheques for investments. This would never happen in Canada because of disconnect with investors."[59] This disconnect between the decision-making of Canadian investors and the needs of early startups is also evident in the relatively slower decision-making processes of Canadian financers. Interviewees felt that Canadian investors took longer to make their investment decisions. This longer lead time is a mismatch to the realities of early startups. Hassan Jafferi, Founder of Bitnobi and Co-Director of UTEST, shared: "There are very different circumstances for writing cheques in Canada compared to other places like the U.S., Asia, and Europe. We still don't have lead investors who want to make investments quickly — people want to take more time to evaluate a deal — but most startups only have a few months of runway."

Others mentioned differences between Canadian and U.S. investors, including varying metrics to validate an investment, an overall larger risk appetite from American investors due in part to a larger market, and greater clusters of VCs to support startup growth. Kim Tremblay, co-founder of Arctic Wolf, likewise mentioned the relatively conservative nature of Canadian VCs, where they look for products that are already further along, have some sales success, and are well on the way to profitability.[60] Although one founder agreed that Canadian investors take longer to make investment decisions, they shared that, once investors agree to provide funding, Canadian financers are committed to their startups in the long term — whereas U.S. investors may provide larger cheques, but tend to pull out if things do not work as planned.[61]

What about the talent shortage?

A scarcity in cybersecurity talent continues to impact organizations across the globe, with demand far exceeding the cybersecurity workforce available. Approximately 2.7 million cybersecurity professionals are needed to fill the global market demand,[62] with around 25,000 cybersecurity positions left unfilled in Canada.[63]

Surprisingly, Canadian cybersecurity startup founders commonly reported that the talent shortage did not have much of an impact on their work. As one founder put it, "talent is a solvable problem. We can just go elsewhere."[64] Cybersecurity entrepreneurs felt that there are much larger issues hindering their commercialization prospects, and that labour scarcity was not a significant area to prioritize when it came to addressing the commercialization gap.

Lack of cybersecurity expertise and connections among investors

Cybersecurity entrepreneurs felt that Canada's VC landscape lacked cybersecurity expertise. Though interviewees felt programs offered by incubators and accelerators were helpful in advancing their companies, few offered cyber-specific expertise to assist ventures in accessing funding.

This lack of subject matter understanding impacts the ability of investors to evaluate startups, in turn leaving them feeling unconfident about investment decisions regarding cybersecurity companies. One participant shared how Canada's investors were mostly generalists, while the U.S. market has more investors with deeper cyber expertise and thus the ability to conduct better risk assessments. A lack of in-depth cybersecurity market expertise makes it difficult for investors to develop trust in cybersecurity startups seeking funding. This lack of understanding and trust makes it difficult for investors to agree to support cyber entrepreneurs. As one roundtable participant put it, "you can't root for tech that you don't understand."

Scarce cybersecurity knowledge also impacts the funding decisions made by government bodies. In their discussion on Canada's tech scale-ups, the Council of Canadian Innovators (CCI) highlighted how the CRA can be misguided on how innovative technologies are developed. This knowledge gap puts early tech businesses at a disadvantage since some of their R&D activities may be deemed ineligible for tax credits by auditors, even though these activities may be vital for the advancement of their innovations.[65]

Founders are also looking to the U.S. to access investors with both expertise and more connections to networks of cybersecurity industry experts. A 2022 report by Canada's Information and Communications Technology Council (ICTC) found that, "while seeking

international investment might result in a company leaving Canada, it also gives that company access to more experienced partners and bigger markets."[66] One cybersecurity startup founder shared that, "even among those who provide cyber funds, startups would rather get foreign funds who have the cyber connections and expertise."[67] Zighra Co-Founder Deepak Dutt echoed similar sentiments: "Founders need those investor supports. It's not just money — it's a need for investors who understand the cybersecurity enterprise space. It's about having these support systems that help you move from Seed to Series A, B, C and closing the gap."[68] With a more mature cybersecurity market, the U.S. has developed a larger body of cybersecurity industry experts who can provide valuable guidance and networks for entrepreneurs. As a result, cybersecurity startups have turned to the U.S., where they can find more specialized investors who can provide both funding and access to valuable networks.

> "Founders want not just money, but also the ability for investors to introduce you to people. This avenue is very ripe in the U.S. but not in Canada."
>
> — Joe Cummins, CybernetIQ

Struggles to secure early adopters

Pivotal to the survival of early startups is securing their first clients; however, Canadian startups are finding a lack of support in finding initial customers. Beauceron Security Co-Founder and CEO David Shipley shared that, although Canada is effective at supporting innovations from conception to product development, "there's a gap in getting it into the hands of early customers who will say yes."[69] Closing this gap is necessary for developing a sustainable startup ecosystem, as securing early adopters can accelerate growth by giving startups access to the much needed capital, feedback and referrals that come with early deals.

Among all of the cybersecurity startups that we spoke with, a vast majority found their first set of customers organically through existing connections or personal referrals, including past managers, partners and clients from previous work experiences. Mathieu Lavoie, Co-Founder of Flare Systems, shared that their company's first sales and hires "started with contacts who trusted us from before."[70] Styx Intelligence Founder Karim Ladha also found that the pre-established trust between himself and his existing connections allowed him to secure initial sales: "My early adopters knew me, the work that I have done, and had trust in me."[71]

This finding is concerning since not all potential entrepreneurs have the advantage of an established pre-existing network. It is unsustainable for startups to rely solely on their personal connections in order to scale and successfully commercialize. Although

incubators, accelerators and international trade offices can help bridge this gap, several founders shared the view that Canadian ones were not helpful in securing their initial customers. Although these organizations allowed founders to meet and present to potential customers, entrepreneurs found that little came out of these endeavours. The inability to establish deals with these potential clients may be a symptom of Canada's aforementioned risk-averse culture, whereby buyers are unwilling to be the first purchasers of early products.

Procurement hurdles

One potential way to address the issue of hesitant early-adopters is for governments to act as the first-buyers of early startup products. A recent study by the UK's Department for Digital, Culture, Media and Sport found that cybersecurity companies in the country reported public procurement as playing a key role in their growth and scaling.[72] Government contracts can also help startups build more credibility in the market in order to attract future customers.[73] Beyond its ability to help propel the commercialization of cybersecurity innovations, public procurement of cybersecurity products also has national security implications. One startup founder shared: "We need to take a deliberate approach for cybersecurity procurement. If we don't maintain our own national capacity in cyber, we're at the mercy of other countries."[74]

Despite the potential for government agencies and offices to act as initial customers for cybersecurity startups, Canada's public procurement processes often remain too time-consuming and arduous for smaller companies. Funded by taxpayers, governments understandably have to practice due diligence in their vendor selection in order to reduce risk. Although founders recognized this, they also felt that public procurement processes have higher barriers than what is necessary. Individuals found that government RFPs for cybersecurity services typically included multiple required certifications that are both expensive to achieve and seemed unnecessary for the contract. In addition, dealing with the paperwork and slow pace of public procurement processes has dissuaded cybersecurity startups from public procurement.

Several interviewees urged Canada's public procurement processes to better favour cybersecurity products developed by Canadian companies. One founder shared that they had an easier time getting procured by the U.S. government, while the Canadian government declined to support their product.[75] Despite public procurement's potential as a driver for startup development, Canada is currently leaving this opportunity unharnessed.

The IP dilemma

IP protection has often been touted as key to a startup's growth and commercialization, as well as the strengthening of the Canadian innovation ecosystem.[76] Recognized by both the government and existing literature, patents are tools to protect inventions, incentivize innovation and growth through the protection of ideas, and enable entrepreneurs to receive the full economic benefits of their product.[77] Patents have also been noted as an indicator of value to venture capitalists, making it easier for entrepreneurs to obtain funding.[78] Ontario's Expert Panel on Intellectual Property

noted that, without appropriate supports for startups to protect their IP, and for knowledge from academic institutions to be translated into workable knowledge, "the knowledge created on Ontario campuses is often left on academic shelves or licensed and/or sold at a development stage that significantly limits the returns to Ontario's economy."[79]

Some interviewees pointed out that governments have begun to notice the need for IP supports, and the range of recently introduced programs and initiatives are reflective of this effort. Federal government efforts include the ElevateIP program, announced in Budget 2021, holding workshops, programs and learning opportunities for startups to develop IP strategies, as well as providing Canadian IP resources for small businesses.[80] Provincial government efforts, such as IP Ontario, are similar to the federal government's efforts helping businesses in the province access IP support.[81] Ontario's Commercialization Mandate Policy Framework has been introduced to assist the commercialization of knowledge from academic institutions, while the Intellectual Property Governance Framework and New Intellectual Property Metrics for Innovation Partners seeks to oversee provincially-funded innovation partners' IP practices.[82]

Lack of incentive to protect IP

Despite efforts by the government and startup ecosystem to support IP protection, a common sentiment shared throughout multiple interviews, and found in some of the literature, was the lack of incentive to protect IP. Barriers mentioned included the amount of time needed to be devoted to file, high costs to access and enforce patents for smaller firms, the diminishing performance benefit of a patent, lack of familiarity with the patent process, and disbelief in the usefulness of having IP protection.[83] In sharing their experiences, some interviewees mentioned that their personal incentive to apply was more for the optics of investors and potential purchasers, rather than the actual intention to protect their product. Others explained that IP theft would happen regardless of whether a product was patented, pointing to the power larger firms and nation state actors have if they wanted to steal IP from their companies. Faud Khan, Founder and Chief Security Analyst of TwelveDot, also shared the difficulty and inherent risk in being a startup, balancing the interest of wanting to share the invention with potential investors or companies, not demanding to sign a non-disclosure agreement, and still wanting to protect the idea from being stolen by bigger companies.[84] Throughout all the interviews, founders had varied opinions on the usefulness of IP protection, as well as further suggestions for how governments can better support startups with IP protection.

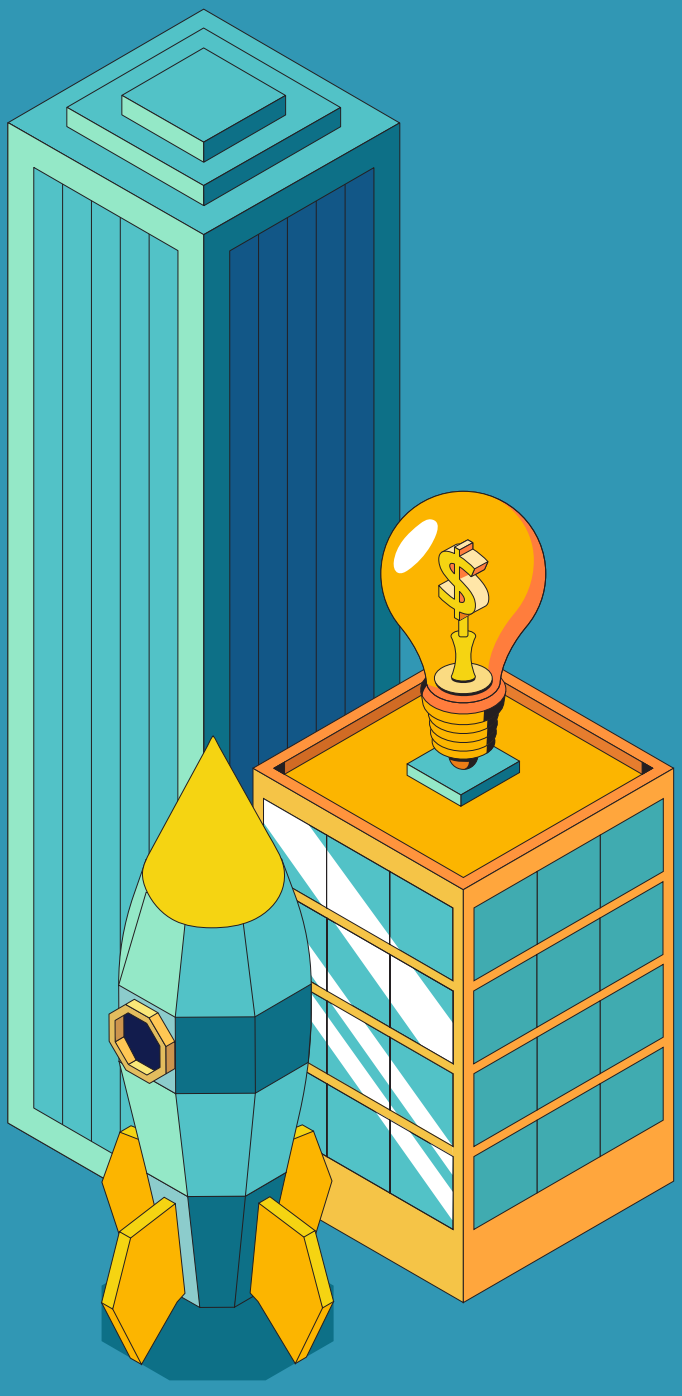
> "There's a lot of onus on startups to invest in these ideas, yet there is no plan on how to protect IP, expand on it, and scale up in commercialization."
>
> — Roundtable participant

Diversity and inclusion

Another commonly cited barrier to startup commercialization is the lack of diversity in the cybersecurity sector. One participant shared that under-represented groups such as women and non-binary individuals, racialized groups, and Indigenous communities struggle to attract funding and clients for their entrepreneurial efforts. Another expert shared their personal difficulties in finding funding and clients as a visible minority. Although networks can be significantly helpful for entrepreneurs to access potential clients, investors and helpful information, under-represented groups such as Black women, immigrants and Indigenous entrepreneurs report a lack of networks as one of their barriers to success.[85]

Another issue is the predominance of white male individuals in the venture capital space.[86] In 2019, 18% of partners at Canadian VC firms identified as visible minorities and only 11% of VC firm partners identified as women.[87] Funding opportunities may be impacted as a result of racial bias among undiverse investment teams. One study found that Black business owners were significantly less likely to receive full financing compared to those who were white, despite having strong personal credit.[88]

Taking Action



05

Taking Action

Recognizing the obstacles that Canadian startups continue to face in their journey to commercialization, the following section highlights the need for multisectoral collaboration and an organized, targeted approach to improving Canada's cyber innovation ecosystem. In order to develop the Canadian cyber innovation ecosystem to support the growth of more home-grown startups, we recommend several key areas for the innovation ecosystem to focus on:

1. Connecting startups to early adopters;
2. Lowering IP protection costs;
3. Closing the risk-aversion gap; and
4. Encouraging diversity.

Connecting startups to early adopters

Stakeholders involved: governments, incubators and accelerators, industry

Early adopters of startup products are vital to their growth and success, but more work needs to be done to successfully connect Canadian cybersecurity entrepreneurs with potential buyers.

Enhancing government innovation programs

Government innovation programs can bring a larger focus on securing government contracts with startup companies. Since cybersecurity plays a major role in national security, Canada can adopt an approach to cybersecurity innovations similar to what the U.S. has done through innovation programs such as In-Q-Tel, which works to realize mutual benefits for both startups and the federal government. Through providing funding, expertise, feedback and access to government partners, In-Q-Tel helps startups commercialize their products and secure early adopters, while also developing emerging technologies that can be leveraged by the government for national security purposes.[89] This could include a dedicated focus in areas where Canada has unique strengths, such as quantum technologies.

Although Canada's existing Innovation for Defence Excellence and Security program (IDeAS) currently includes opportunities for program participants to present their products to DND, CAF and other government agencies, our interviewees shared that the current process is often too slow for early startups that cannot afford delayed cash flow. One founder felt that the IDeAS program did not offer enough funding considering the amount of effort the program requires from innovators, in addition to the lack of guaranteed customers from the endeavour.

Similar to the IDeAS program is Innovative Solutions Canada (ISC), an initiative run by Innovation, Science and Economic Development Canada (ISED). With less of a focus on defence technologies, ISC provides funding for innovators to build their prototypes and test their products.[90] Government departments can participate in the program

in two ways: they can put out challenges for which innovators can develop solutions; and they can test innovations that have yet to be introduced to the market. Although a promising model, ISC is still lacking in size and capacity. In 2020, only three businesses completed two out of three phases of the ISC's Challenge Stream, whereby innovators develop a solution for a government agency.[91] While ISC awarded close to 190 grants and contracts totalling approximately $77 million CAD in 2020, the U.S.'s Small Business Innovation Research Program (SBIR) provided 7,306 awards valued around $3.9 billion USD in the same year.[92]

While the Canadian programs serve a much smaller Canadian domestic market, the contrast demonstrates the opportunity for proportionately increasing the funding and investment size of Canada's innovation programs. In all, enhancing the IDeAS and ISC programs to strengthen the pathway for cybersecurity startups to secure government contracts could help improve the commercialization prospects of these startups.

Exploring better ways of procurement

Government procurement has the potential to be a driver for startup commercialization, but has been long known as an arduous process that can put startups at a disadvantage during competitions. A public procurement model for certain cybersecurity services could be piloted that provides greater advantages for Canadian companies for the purposes of enhancing national security. Policies that require major cybersecurity contract winners to undertake a portion of business activity with small- and medium-sized businesses in Canada could also support Canadian commercialization, similar to the ISED's Industrial and Technological Benefits policy applied to major defence contracts. Modifying procurement processes introduces practical and regulatory challenges, particularly mitigating potential risks of retaliatory trade sanctions for preferential treatment[93] — though all of Canada's trade agreements have exceptions for procurements related to national security that could potentially be leveraged.[94] Using a pilot approach may help address the risk-averse nature of government procurement by allowing new approaches to be tested before any full-scale adoption.[95] This is important, since support and buy-in from government procurement employees help contribute to successful program changes.[96]

To relieve procurement barriers in the short term, governments can also provide better services to support entrepreneurs through the procurement process. This can look like implementing case workers or a reliable point of contact to provide startups with information on the status of their procurement, as well as answering questions that entrepreneurs may have. This could be modelled on new concierge approaches being used for scale-ups federally and in B.C.[97]

Developing a product validation model

Ecosystem players should convene to examine the feasibility and potential structure of a product validation model. Since trust and credibility are vital for the adoption of cybersecurity products, a mechanism for validating and vetting cybersecurity startup products can help signal these important features, similar to the model deployed nationally for cybersecurity certification of small and medium enterprises.

The UK government is currently developing a process for publicly validating the cybersecurity of domestically-created commercial technologies. The National Cyber Security Centre (NCSC) Technology Assurance strategy seeks to cultivate confidence in UK tech innovations.[98] Through testing products and evaluating its cybersecurity measures, the NCSC Technology Assurance program is meant to convey to domestic and international buyers that the assured technologies are reliable, reputable and secure.[99] However, many considerations will need to be addressed when developing an assurance model for cybersecurity innovations. The UK's previous scheme for assessing security products began in 2014, but was terminated in 2019 because it failed to support a broad enough range of customers.[100] Learning from this experience, the NCSC Technology Assurance scheme will aim to cater to a broad range of use cases, technologies and contexts.[101] The new assurance model will also take a principles-based approach rather than a prescriptive one, so that the program doesn't leave out innovations that don't fit a rigid model. A product validation model designed with flexibility in mind is befitting for cybersecurity innovations, given that cybersecurity technologies can vastly differ from one another in terms of systems, use cases, intended users, and more.

In all, a reputable product validation model can confirm to investors and buyers that startup products are meeting industry and regulatory standards. Such a confirmation can help improve the chances of startups receiving investment and securing early adopters. It could also help facilitate incubators, accelerators and trade offices in connecting potential enterprise customers with startups with greater confidence, while addressing the barriers faced by diverse entrepreneurs, who are often without existing customer networks. The UK's Department for Digital, Culture, Media and Sport (DCMS) reflected this sentiment, listing one of the key factors driving investors' investment decisions in 2021 as "validation of their product/service from sophisticated buyers", as this addressed the challenge of "validating the uniqueness and defensibility of cyber technologies."[102] An interviewee in the DCMS report stated the potential ability to drop revenue limits and requirements in the case where a product is validated and vouched for in the cyber industry, which would ultimately drop barriers to finding investment.[103]

Lowering IP protection costs

Stakeholders involved: governments, incubators and accelerators

Dedicated funding streams to promote IP protection should be introduced in order to better incentivize cybersecurity entrepreneurs to protect their IP. As recommended by Ontario's Expert Panel on Intellectual Property, providing more resources for IP protection and commercialization can bring generous returns to Canada.[104] As early startups have limited cash flow, such funding can better encourage entrepreneurs and researchers to protect their IP without implicating their finances.

Canada's existing Scientific Research and Experimental Development (SR&ED)

tax incentives can be reformed to help compensate IP ownership costs. The Canadian Council of Innovators has suggested that activities related to IP protection should be eligible expenses as a way to encourage Canadian startups to pursue IP ownership.[105] Such measures can help lower the net cost of patent filing, improve incentivization of IP ownership efforts, and help companies and Canada realize the long-term benefits related to the protection of intangible assets.

At the same time, new measures should be considered to ensure that IP developed using public R&D funds are retained in Canada. Countries like the U.S., UK and Israel have various mandates in place to ensure that ownership of IP derived from public funds remains in the country, or else financial penalties are implemented against the company that exports their IP.[106] Measures such as these would ensure that Canada benefits from the economic returns from Canadian innovations.

Closing the risk-aversion gap

Stakeholders involved: government, industry, investors, non-profit intermediaries, accelerators and incubators, academia

Canada's risk averse culture needs to be bridged in order to ensure that cybersecurity startups can secure investors and buyers without having to resort to opportunities outside of Canada.

Targeted public investment

The Canadian government can play a role in this area by stepping in to provide support for innovative cybersecurity startups when investors decline ventures. This approach has been emphasized in the U.S., with In-Q-Tel CEO and President Christopher Darby emphasizing to Congress how "the government has an obligation to invest" when VCs fail to invest in technologies that do not fit their proven models.[107] The U.S. Government's Small Business Innovation Research Program (SBIR) is one demonstration of these efforts. Their funding for early-stage companies with commercialization prospects are designed to be comparable to private sector investments and are meant to be an indication of "acceptance of greater risk in support of agency missions."[108] Public risk capital is necessary since the ROI horizons may be longer for cybersecurity innovations. The Canadian government can take a similar approach to the U.S. by stepping up to accept greater risk in support of cybersecurity startups, and the benefits that their innovations bring to the economy and national defense.

Growing cyber industry expertise

Education and knowledge-building opportunities could help develop a better understanding of cybersecurity innovations — in turn improving their ability to evaluate cybersecurity startups when making funding decisions. Startups, industry, academic institutions, non-profit intermediaries, and accelerators and incubators all play a role in helping to close the cybersecurity knowledge gap. Stakeholders can convene, and share expertise and guidance through resources, roundtables, conferences, presentations and other methods of knowledge sharing.

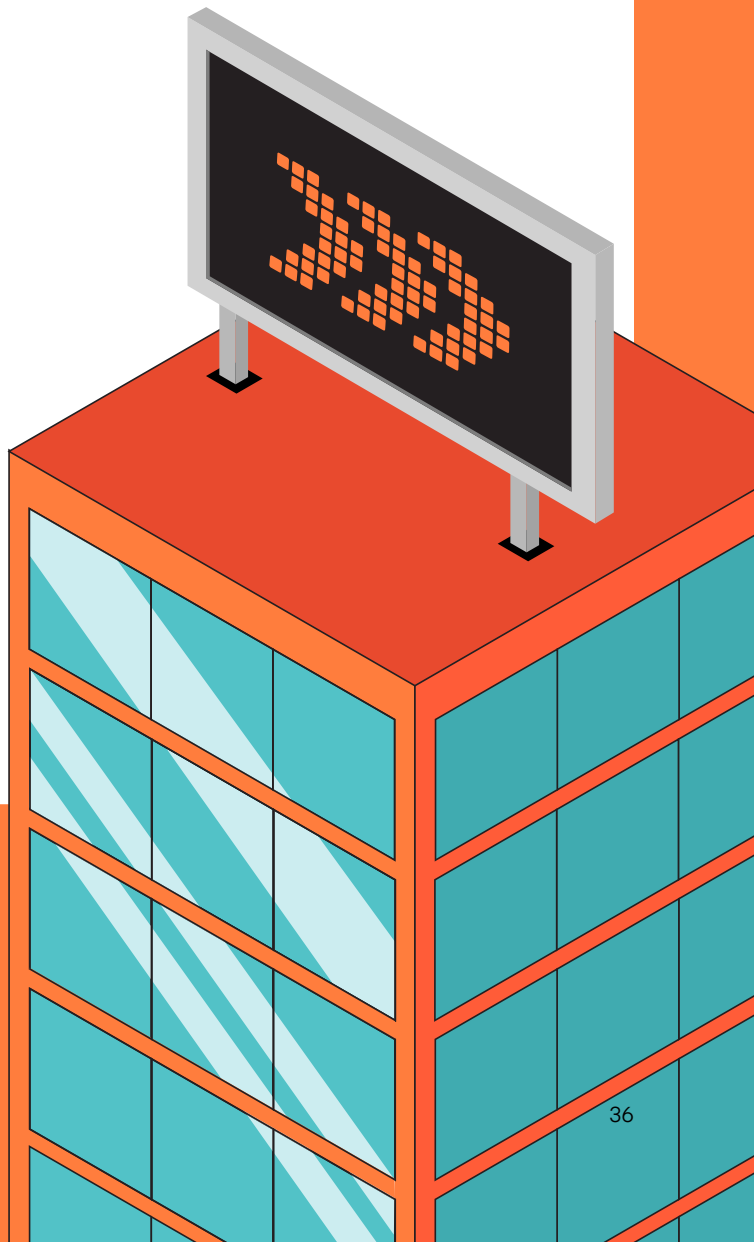
Informative resources for investors to identify worthy cyber startups in which to invest, as well as resourcing for auditors to understand how tech is developed, can waive the risk of technology being eliminated from funding and further development. The Canadian Council of Innovators has proposed specific auditor education on assessing the needs, operations and process flows of modern technology companies, in order to appropriately support companies and evaluate technologies.[109] This may be an opportunity for government bodies and non-profit intermediaries to contribute educational efforts for auditors. Closing the knowledge gap between investors and auditors, and the technology they are evaluating, will allow for a fairer playing field for all startups to access the support they need.

Data sharing

In order to facilitate coordination and inform better decision-making, knowledge gaps between ecosystem players need to be reduced. A robust data strategy that encourages data collection and information sharing among ecosystem members can help stakeholders identify gaps and improve their business case for startup support.

Roundtable participants highlighted a need for more statistics related to the demand side of the cybersecurity market. Several participants felt that the Canadian Centre for Cyber Security and Statistics Canada both hold valuable data related to Canada's cybersecurity landscape that could be more proactively shared.

Cybersecurity scale-ups and other companies that have experienced successful commercialization can also contribute back to the startup system by sharing their knowledge and experiences to early startups.



Encouraging diversity

Stakeholders involved: government, investors, academia

Strengthening the cybersecurity startup ecosystem and national security capabilities can be realized through the diversification of involvement and perspectives from ecosystem players themselves. Diverse representation from under-represented groups such as women and non-binary individuals, racialized groups and Indigenous communities is vital to continue to encourage entrepreneurial efforts and commercialization. Although encouraging diversity must be reinforced by all ecosystem stakeholders, two key players with pivotal impact are academia and investors.

The cultivation and sourcing of diverse talent for the cybersecurity ecosystem in Canada is heavily reliant on academic institutions around the country. Although initiatives such as the *Cyber. Right. Now.* campaign recognize the issue of building Canada's diverse workforce, top talent has often been poached, or has left to work abroad, with nearly two-thirds of Canadian-educated software engineering students leaving to work outside of Canada.[110] In addition to addressing the exit of diverse domestic talent, another consideration has been to identify the diversity of background and skills needed in the industry, which may not fit neatly into the traditional, monolithic IT backgrounds.[111] Gathering data to reframe existing skill sets and combining diverse groups of people could assist in filling in existing workforce gaps as well.[112] One initiative seeking to add diversity among cybersecurity talent is the Rogers Catalyst's Accelerated Cybersecurity Training Program. This program provides heavily subsidized cybersecurity training for new Canadians, individuals who identify as women or non-binary, people who are underemployed, and those seeking new careers.[113]

The importance of diverse perspectives has also been recognized in the investment sector. VC firms and investment communities have been proven to benefit from diverse perspectives due to the resulting greater creativity generated, and improved financial performance.[114] Similar to diverse talent representation generated in academia, participants mentioned the need for more investors to be involved in the ecosystem, especially with varying levels of expertise in cybersecurity-related matters. More investors with diverse subject matter-related knowledge and understanding would open up the ecosystem to further investment opportunities for startups.

Conclusion

As the internet and digital economy have matured, it has become clear that cybersecurity and digital privacy represent some of the most pressing challenges facing our modern world. In Canada, a cybersecurity innovation ecosystem has emerged to support startups and high-growth firms that assist people, businesses and institutions to secure their devices, systems and data against online threats. Coordinating these groups to foster a more sustainable cybersecurity startup ecosystem can help propel Canada as a global leader, bringing geopolitical, economic and national security benefits. With greater guidance and investment opportunities from government and collaboration across all sectors, Canada has the potential to advance its technological competitiveness within the global economy.

About the Authors

Stephanie Tran is an experienced researcher with over five years of experience analyzing public policy and human rights issues related to digital technologies, with past experience working for the Citizen Lab, Amnesty International Canada, the United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA) and more. She is a trained computer programmer, having earned a Diploma in Computer Programming from Seneca College. She also holds a dual degree Master of Public Policy (Digital, New Technology and Public Affairs Policy stream) from Sciences Po in Paris, and a Master of Global Affairs from the University of Toronto. She earned her BA degree from the University of Toronto specializing in Peace, Conflict and Justice.

Tiffany Kwok is an active researcher in the digital and service delivery realm - from working on modernizing social assistance pathways in the Ontario Public Service, to partaking in research projects both in the public sector (service pathway improvement and digitization in UK healthcare) and the private sector (sociotechnical security in UK railway systems) in Canada and the UK. She has also worked on academic and on-the-ground research, through various roles with the University of Toronto, the City of Toronto's SDFA, and with the NATO Association of Canada. Tiffany holds a BA in Political Science and Urban Studies from the University of Toronto, and is currently completing her MPA in Digital Technologies and Policy from University College London.

Appendix: Project Participants

It is important to note that the varied perspectives of our interview and round-table participants greatly informed this report; however, the statements and recommendations are solely those of the authors. Any errors or omissions in fact or interpretation remain the sole responsibility of the authors.

A list of project participants (who consented to having their names made publicly available) is as follows:

Alex Maheu, Amazon Canada
Chad Peters, Canadian Centre for Cyber Security
Dan Desjardins, Distributed
David Shipley, Beauceron Security Inc.
Deborah Clark-Foster, Ontario Ministry of Economic Development, Job Creation and Trade
Deepak Dutt, Zighra
Faud Khan, TwelveDot
Grant Colhoun, Okanii
Hassan Jaferi, UTEST, Bitnobi Inc
Ian Paterson, Plurilock
James Stewart, TrojAI
Jason Besner, Canadian Centre for Cyber Security
Joe Cummins, CybenetIQ
Karim Ladha, Styx Intelligence
Kim Tremblay, Arctic Wolf
Mark Maybank, Maverix Private Equity
Mathieu Lavoie, Flare Systems Inc.
Nick Schiavo, Council of Canadian Innovators
Prat Sureka, Communitech
Robert Beggs, DigitalDefence
Robert Gordon, Canadian Cyber Threat Exchange
Robert Luke, eCampusOntario
Rod Schatz, McElhanney
Scott Wright, Click Armor
Stephen Goddard, TrojAI
Tim Stupich, CANARIE
Ulrike Bahr-Gedalia, Canadian Chamber of Commerce

References

[1] Public Safety Canada. (2022, July 21). *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*. Public Safety Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx#s4

[2] HHRG-116-IG10: The Unseen Conflict: Strategic Technology Competition: Hearings before the Strategic Technology and Advanced Research Subcommittee of the House Permanent Select Committee on Intelligence. Testimony of Mr. Christopher Darby. (2020). https://www.congress.gov/116/meeting/house/110489/witnesses/HHRG-116-IG10-Bio-DarbyC-20200212.pdf

[3] Araya, D., & Mavinkurve, M. (2022). Emerging Technologies, Game Changers and the Impact on National Security (No. 9; Reimagining a Canadian National Security Strategy). Centre for International Governance Innovation. https://www.cigionline.org/publications/emerging-technologies-game-changers-and-the-impact-on-national-security/

[4] Bahr-Gedalia, U. & Dickman, M. (2021, September). Can Canada be a global cybersecurity leader? Innovating Canada. https://www.innovatingcanada.ca/business-and-economy/can-canada-be-a-global-cybersecurity-leader/; Pitchbook. (2022). Retrieved July 18, 2022 from Pitchbook database.

[5] Brown, J. (2021). Cybersecurity Research Report 2021. Crunchbase. https://about.crunchbase.com/cybersecurity-research-report-2021/

[6] Expert Panel on Intellectual Property. (2020). *Intellectual Property in Ontario's Innovation Ecosystem*. Ministry of Colleges and Universities. https://www.ontario.ca/document/report-intellectual-property-in-ontarios-innovation-ecosystem

[7] **Early stage startups** are companies that are still in development, including those between seed to series B funding stages. **Scale-up companies** have experienced an average annual growth rate greater than 20 percent over the past three years, with at least 10 employees at the beginning of the period. Unicorns are highly successful, private startup companies with a valuation of over $1 billion.

Adhanan, E. What are the three stages of a startup? Silicon Valley Bank. https://www.svb.com/startup-insights/startup-growth/what-are-the-three-stages-of-a-startup.

Embroker Team. (2022, October). Unicorn Startups by Industry and Lessons from the $1B+ Club. Embroker. https://www.embroker.com/blog/unicorn-startups/.

Song, M. & Bérubé, C. (2021). *Canadian startups: Growth and Scale-up Transitions*. Innovation, Science and Economic Development Canada. https://www.ic.gc.ca/eic/site/061.nsf/eng/h_03132.html.

[8] Mandel, C. (2022, June 9). Flare Systems eyes US Expansion following $9.5 Million Series A Funding. *Betakit*. https://betakit.com/flare-systems-eyes-us-expansion-following-9-5-million-series-a-funding/.

[9] Prairie, E. (2022, August 9.) Arctic Wolf Named to the 2022 Forbes Cloud 100. *Arctic Wolf*. https://www.globenewswire.com/news-release/2022/08/09/2495095/0/en/Arctic-Wolf-Named-to-the-2022-Forbes-Cloud-100.html.

[10] Denney, S., Southin, T., & Wolfe, D. A. (2021). Entrepreneurs and cluster evolution: The transformation of Toronto's ICT cluster. Regional Studies, 55(2), 196–207. https://doi.org/10.1080/00343404.2020.1762854

[11] CBRE Research. (2022). Scoring Tech Talent 2022. CBRE. https://www.cbre.com/insights/books/scoring-tech-talent-2022

[12] Matthews, M., & Rice, F. (2022). Context Matters: Strengthening the Impact of Foreign Investment on Domestic Innovation. Information and Communications Technology Council (ICTC). https://www.digitalthinktankictc.com/ictc-admin/resources/admin/fdi-ip-canadian-innovation-2022.pdf

[13] *Intellectual Property Commercialization Policy and Procedures | Vice-Principal (Research)*. (2022, March 31). Queen's University. https://www.queensu.ca/vpr/news/ip-policy

[14] Innovation, Science and Economic Development Canada. (2022, May 11). Programs and Initiatives. Government of Canada. https://www.ic.gc.ca/eic/site/icgc.nsf/eng/h_07654.html.

[15] National Defence. (2021, July 2). Innovation for Defence Excellence and Security (IDEaS). Government of Canada. https://www.canada.ca/en/department-national-defence/programs/defence-ideas.html; National Defence. (2021, July 6). Test drives. Government of Canada. https://www.canada.ca/en/department-national-defence/programs/defence-ideas/element/test-drives.html

[16] Innovation Government of Canada. (2022, September 27). Industrial and Technological Benefits—Home [Home page;]. Innovation Government of Canada. https://ised-isde.canada.ca/site/industrial-technological-benefits/en/industrial-and-technological-benefits

[17] Public Safety Canada. (2022, July 21). *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*. Public Safety Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx#s4

[18] Silicon Valley Bank. (2019). Canada Startup Outlook 2019: Key Insights from the Silicon Valley Bank Startup Outlook Survey. https://www.svb.com/globalassets/library/uploadedfiles/content/trends_and_insights/reports/startup_outlook_report/canada/svb-suo-canada-report-2019.pdf

[19] Ferreira, V. (2019, March 20). Canada's cybersecurity firms keep turning to the U.S. for funding, leaving us without a homegrown leader. *Financial Post*. https://financialpost.com/technology/canada-cybersecurity-firms-u-s-funding.

[20] Richards, R. (2021, June 10). *Accelerators Vs Incubators: How to Choose the Right One*. Mass Challenge. https://masschallenge.org/article/accelerators-vs-incubators

[21] Ibid.

[22] *ABOUT CCTX*. (n.d.). [CCTX]. Canadian Cyber Threat Exchange – CCTX – Informing Canadian Business. Retrieved October 13, 2022, from https://cctx.ca/about-cctx/

[23] *Standards*. (n.d.). CIO Strategy Council. Retrieved October 13, 2022, from https://ciostrategycouncil.com/standards/

[24] PitchBook Emerging Tech Research (2022). Retrieved from Pitchbook database.

[25] Ferrara, A., Karp, A., & Tarnopol, C. (2022, January 31). Cybersecurity startup trends of 2022. Bessemer Venture Partners. https://www.bvp.com/atlas/2022-cybersecurity-startup-trends

[26] Brown, J. (2021). Cybersecurity Research Report 2021. Crunchbase. https://about.crunchbase.com/cybersecurity-research-report-2021/

[27] CB Insights. (2022, August 30). *State of Cybersecurity Q2'22 Report*. CB Insights Research. https://www.cbinsights.com/research/report/cybersecurity-trends-q2-2022/

[28] Metinko, C. (2022, October 11). Cybersecurity Funding Continues Slide In Q3. *Crunchbase News*. https://news.crunchbase.com/cybersecurity/cyber-funding-pullback-q3-2022-unicorn/

[29] Stupp, C. (2019). CISOs Search for Startup Gold in Mountain of Cybersecurity Pitches; Talent shortage, startups' AI prowess mean executives feel compelled to sort through vendor offers. WSJ Pro Cyber Security, https://www.wsj.com/articles/cisos-search-for-startup-gold-in-mountain-of-cybersecurity-pitches-11573036200

[30] Pitchbook (2022).

[31] Ibid.

[32] *Cybersecurity—Canada | Statista Market Forecast*. (n.d.). Statista. Retrieved October 14, 2022, from https://www.statista.com/outlook/tmo/cybersecurity/canada

[33] Crunchbase. (2021). *Report: The Rise of Global Cybersecurity Venture Funding*. Crunchbase. https://about.crunchbase.com/cybersecurity-research-report-2021/.

Statista. (2022). *Cybersecurity – United States*. Statista. https://www.statista.com/outlook/tmo/cybersecurity/united-states.

[34] Erbschloe, M. (2017). Threat level red: Cybersecurity research programs of the U.S. government (1st ed.). CRC Press, Taylor & Francis Group. https://doi.org/10.1201/9781315167558

SBIR-STTR. (2014). *The SBIR and STTR Programs*. SBIR-STTR. https://www.sbir.gov/about.

[35] In-Q-Tel. (2022) Innovation on a Mission. In-Q-Tel. https://www.iqt.org/#:~:text=Innovation%20on%20a%20Mission&text=Dedicated%20government%20professionals.,the%20U.S.%20and%20its%20allies.

[36] Erbschloe, M. (2017). Threat level red: Cybersecurity research programs of the U.S. government (1st ed.). CRC Press, Taylor & Francis Group. https://doi.org/10.1201/9781315167558.

[37] Shipley, D. (2022, August 5). [Personal Communication].

[38] Crunchbase. (2021). *Report: The Rise of Global Cybersecurity Venture Funding*. Crunchbase. https://about.crunchbase.com/cybersecurity-research-report-2021/.

Jaghory, D. (2022, June 3). *Cybersecurity in Israel: Fortifying Digital Defenses Amid Elevated Risks*. Global X. https://www.globalxetfs.com/cybersecurity-in-israel-fortifying-digital-defenses-amid-elevated-risks/#:~:text=Israel%27s%20cybersecurity%20sector%20amassed%20%248.84,comparison%20to%202020%27s%20%242.75%20billion.&text=Globally%2C%2040%25%20of%20private%20investments,small%20size%20of%20the%20country.

[39] Crunchbase. (2021). *Report: The Rise of Global Cybersecurity Venture Funding*. Crunchbase. https://about.crunchbase.com/cybersecurity-research-report-2021/.

Statista. (2022). *Cybersecurity – United Kingdom*. Statista. https://www.statista.com/outlook/tmo/cybersecurity/united-kingdom#:~:text=Revenue%20in%20the%20Cybersecurity%20market,US%245.77bn%20in%202022.

[40] Donaldson, S., Crozier, D., Matorell, S., McLaren, I., Douglas, J., & Shah, J. N. (2022). UK Cyber Security Sectoral Analysis 2022. Department for Digital, Culture, Media and Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1055565/Cyber_Sectoral_Analysis_2022_Report_V2.1.pdf

United Kingdom: Record levels of investment for UK's £10.1 billion cyber security sector. (2022, Feb 22). *Asia News Monitor* http://ezproxy.lib.ryerson.ca/login?url=https://www-proquest-com.ezproxy.lib.ryerson.ca/newspapers/united-kingdom-record-levels-investment-uks-£10-1/docview/2630952286/se-2?accountid=13631

[41] Ibid.

[42] Donaldson, S., Crozier, D., Matorell, S., McLaren, I., Douglas, J., & Shah, J. N. (2022). UK Cyber Security Sectoral Analysis 2022. Department for Digital, Culture, Media and Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1055565/Cyber_Sectoral_Analysis_2022_Report_V2.1.pdf.

[43] Gallini, N., & Hollis, A. (2019). To Sell or Scale Up: Canada's Patent Strategy in a Knowledge Economy. IRPP Study 72. Montreal: Institute for Research and Public Policy. https://irpp.org/research-studies/to-sell-or-scale-up-canadas-patent-strategy-in-a-knowledge-economy/

[44] Canada, Parliament. House of Commons Standing Committee on Industry, Science and Technology. (2017). Evidence. 42nd Parl., 1st sess. Rept. 65. https://www.ourcommons.ca/Content/Committee/421/INDU/Evidence/EV9015393/INDUEV65-E.PDF

[45] Harris, R. G., & Royal Commission on the Economic Union and Development Prospects for Canada. (1985). *Trade, industrial policy and international competition*. University of Toronto Press, Royal Commission on the Economic Union and Development Prospects for Canada and the Canadian Government Publishing Centre, Supply and Services Canada, as cited in Wolfe, D. (2017). *Innovation by Design: Impact and Effectiveness of Public Support for Innovation*. Annals of Science and Technology Policy. https://munkschool.utoronto.ca/ipl/files/2017/10/IPL-PAPER-2017-3.pdf

[46] Matthews, M., & Rice, F. (2022). Context Matters: Strengthening the Impact of Foreign Investment on Domestic Innovation. Information and Communications Technology Council (ICTC). 6. https://www.digitalthinktankictc.com/ictc-admin/resources/admin/fdi-ip-canadian-innovation-2022.pdf

[47] Khan, F. (2022, August 4). [Personal Communication].

[48] Paterson, I. (2022, August 16). [Personal Communication].

[49] Duruflé, G., Hellmann, T., & Wilson, K.E. (2017). From startup to Scale-up: Examining Public Policies for the Financing of High-growth Ventures. Bruegel. http://ezproxy.lib.ryerson.ca/login?url=https://www.proquest.com/reports/startup-scale-examining-public-policies/docview/1894454907/se-2?accountid=13631

[50] Matthews, M., & Rice, F. (2022). Context Matters: Strengthening the Impact of Foreign Investment on Domestic Innovation. Information and Communications Technology Council (ICTC). 8. https://www.digitalthinktankictc.com/ictc-admin/resources/admin/fdi-ip-canadian-innovation-2022.pdf

[51] Jaferi, H. (2022, August 5). [Personal Communication].

[52] Duruflé, G., Hellmann, T., & Wilson, K.E. (2017). From startup to Scale-up: Examining Public Policies for the Financing of High-growth Ventures. Bruegel. http://ezproxy.lib.ryerson.ca/login?url=https://www.proquest.com/reports/startup-scale-examining-public-policies/docview/1894454907/se-2?accountid=13631

[53] Rowe, Andrea, et al. (2019). Scaling startups: Challenges in Canada's Innovation Ecosystem. The International Society for Professional Innovation Management (ISPIM). https://www.proquest.com/conference-papers-proceedings/scaling-startups-challenges-canadas-innovation/docview/2220698841/se-2

[54] Business Development Bank of Canada. (2015). High-Impact Firms: Accelerating Canadian Competitiveness. Business Development Bank of Canada. 11. https://www.bdc.ca/globalassets/digizuite/10492-high-impact-firms-accelerating-canadian-competitiveness.pdf

[55] Advisory Council on Economic Growth. (2017, Feb). Unlocking Innovation to Drive Scale and Growth. Advisory Council on Economic Growth. https://www.budget.gc.ca/aceg-ccce/pdf/innovation-2-eng.pdf.

[56] Colhoun, G. (2022, August 2). [Personal Communication].

[57] Goddard, S. & Stewart, J. (2022, August 8). [Personal Communication].

[58] Paterson, I. (2022, August 16). [Personal Communication].

[59] Cummins, J. (2022, August 1). [Personal Communication].

[60] Tremblay, K. (2022, August 8). [Personal Communication].

[61] Lavoie, M. (2022, August 10). [Personal Communication].

[62] National Institute of Standards and Technology. (2021). *Cybersecurity Workforce Demand*. NIST. https://www.nist.gov/document/workforcedemandonepager2021finalpdf.

[63] *(ISC)2 Cybersecurity Workforce Study 2021* ((ISC)2 Cybersecurity Workforce Study). (2021). (ISC)2. https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

[64] Roundtable participant. (2022, September 23). [Personal communication].

[65] Schiavo, N., & Kamat, A. (2022). *Modernizing SR&ED to Support Canada's "Scale-Up" Companies*. Council of Canadian Innovators. https://8440337.fs1.hubspotusercontent-na1.net/hubfs/8440337/Policy%20Brief%20-%20SR%26ED%20September%202022-1.pdf

[66] Matthews, M., & Rice, F. (2022). *Context Matters: Strengthening the Impact of Foreign Investment on Domestic Innovation*. Information and Communications Technology Council (ICTC). https://www.digitalthinktankictc.com/ictc-admin/resources/admin/fdi-ip-canadian-innovation-2022.pdf

[67] Paterson, I. (2022, August 16). [Personal Communication].

[68] Dutt, D. (2022, August 5). [Personal Communication].

[69] Shipley, D. (2022, August 5). [Personal Communication].

[70] Lavoie, M. (2022, August 10). [Personal Communication].

[71] Ladha, K. (2022, August 11). [Personal Communication].

[72] Donaldson, S., Crozier, D., Matorell, S., McLaren, I., Douglas, J., & Shah, J. N. (2022). UK Cyber Security Sectoral Analysis 2022. Department for Digital, Culture, Media and Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1055565/Cyber_Sectoral_Analysis_2022_Report_V2.1.pdf

[73] Abramowitz, T., Christmann, T., McKenzie, A., Pretorius, E., & Lyst, C. A. (2021). Innovation at scale: Establishing Canada as a global leader. Deloitte. 14. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/fcc/ca-en-innovation-at-scale-establishing-canada-as-a-global-leader.pdf

[74] Shipley, D. (2022, August 5). [Personal Communication].

[75] Cummins, J. (2022, August 1). [Personal Communication].

[76] Matthews, M., & Rice, F. (2022). Context Matters: Strengthening the Impact of Foreign Investment on Domestic Innovation. Information and Communications Technology Council (ICTC). https://www.digitalthinktankictc.com/ictc-admin/resources/admin/fdi-ip-canadian-innovation-2022.pdf

[77] Canada, Parliament. House of Commons Standing Committee on Industry, Science and Technology. (2017). Evidence. 42nd Parl., 1st sess. Rept. 65. https://www.ourcommons.ca/Content/Committee/421/INDU/Evidence/EV9015393/INDUEV65-E.PDF

Collette, E., Santilli, D., Nabavi, M.-A., Barski, G., & Domerçant, R. (2020). IP Canada Report 2020—Canadian Intellectual Property Office. Canadian Intellectual Property Office. https://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/h_wr04873.html

Gallini, N., & Hollis, A. (2019). To Sell or Scale Up: Canada's Patent Strategy in a Knowledge Economy. IRPP Study 72. Montreal: Institute for Research and Public Policy. https://irpp.org/research-studies/to-sell-or-scale-up-canadas-patent-strategy-in-a-knowledge-economy/

[78] Ibid.

[79] Expert Panel on Intellectual Property. (2020). Intellectual Property in Ontario's Innovation Ecosystem. Ministry of Colleges and Universities. https://www.ontario.ca/document/report-intellectual-property-in-ontarios-innovation-ecosystem

[80] Innovation, Science and Economic Development Canada. (2022). ElevateIP. Government of Canada. https://ised-isde.canada.ca/site/elevateip/en.

[81] Innovation, Science and Economic Development Canada. (2022). ElevateIP. Government of Canada. https://ised-isde.canada.ca/site/elevateip/en.

Ontario Makes Significant Progress on Intellectual Property Action Plan. (2022, March 3). News.Ontario.Ca. https://news.ontario.ca/en/backgrounder/1001686/ontario-makes-significant-progress-on-intellectual-property-action-plan

[82] Ontario Makes Significant Progress on Intellectual Property Action Plan. (2022, March 3). News.Ontario.Ca. https://news.ontario.ca/en/backgrounder/1001686/ontario-makes-significant-progress-on-intellectual-property-action-plan

[83] Gallini, N., & Hollis, A. (2019). To Sell or Scale Up: Canada's Patent Strategy in a Knowledge Economy. IRPP Study 72. Montreal: Institute for Research and Public Policy. https://irpp.org/research-studies/to-sell-or-scale-up-canadas-patent-strategy-in-a-knowledge-economy/

Denney, S., Vu, V., & Kelly, R. (2021). Into the Scale-up-verse: Exploring the landscape of Canada's high-performing firms. Brookfield Institute. https://brookfieldinstitute.ca/scale-up-verse

[84] Khan, F. (2022, August 4). [Personal Communication].

[85] Cukier, W., Mo, G. Y., Chavoushi, Z. H., Borova, B., & Osten, V. (2022). *The State of Women's Entrepreneurship in Canada 2022*. Women Entrepreneurship Knowledge Hub. https://wekh.ca/wp-content/uploads/2022/03/WEKH_State_of_Womens_Entrepreneurship_in_Canada_2022.pdf

[86] Deschamps, T. (2021, February 10). *Black entrepreneurs in Canada struggle to raise money from venture capitalists*. Financial Post. https://financialpost.com/entrepreneur/i-dont-want-to-be-a-unicorn-black-founders-struggle-to-raise-venture-capital

[87] *CVCA State of Diversity and Inclusion 2019*. (2019). Canadian Venture Capital and Private Equity Association. https://www.cvca.ca/files/reports/2019-state-of-diversity/CVCA-State-of-Diversity-and-Inclusion-2019.pdf

[88] Jackson, J. (2021, February 2). *The Barriers and Lost Opportunities in Backing Canada's Black Entrepreneurs*. CVCA Central. https://central.cvca.ca/the-barriers-and-lost-opportunities-in-backing-canadas-black-entrepreneurs

[89] In-Q-Tel Engagement. (2022, April 11). U.S. Department of Homeland Security. https://www.dhs.gov/science-and-technology/iqt

[90] Innovation Government of Canada. (2022, September 2). *Innovative Solutions Canada—Home* [Home page;]. Innovation Government of Canada. https://ised-isde.canada.ca/site/innovative-solutions-canada/en/innovative-solutions-canada

[91] Innovation Government of Canada. (2022). *Innovative Solutions Canada: Annual Report 2020–21*. Innovation Government of Canada. https://ised-isde.canada.ca/site/innovative-solutions-canada/en/innovative-solutions-canada-annual-report-2020-21

[92] *Award—Chart | SBIR.gov.* (n.d.). SBIR.Gov. Retrieved October 11, 2022, from https://www.sbir.gov/analytics-dashboard?year%5B%5D=2020

[93] Emanuelli, P. (2022). *"Buy Ontario" scheme a Protectionist Pantomime*. The Procurement Office. https://procurementoffice.com/buy-ontario-scheme-a-protectionist-pantomime/

[94] Emanuelli, P. (2009). *Local Preference in Public Purchasing: Risks and Recommendations: A Whitepaper*. https://s3.amazonaws.com/images.chaptermanager.com/chapters/cd2f8590-ff70-8eca-4c04-88afc4766544/files/local-preference-white-paper-final1.pdf; 3.105. National Security Exceptions, (2021). https://buyandsell.gc.ca/policy-and-guidelines/supply-manual/section/3/105

[95] Huynh, A., Russek, H., & Park, M. (2019). *What's in the Mix: Opportunities + challenges for municipal innovation procurement*. Brookfield Institute. https://brookfieldinstitute.ca/whats-in-the-mix-opportunities-challenges-for-municipal-innovation-procurement

[96] Ibid.

[97] Hemmadi, urad. (2022, August 26). Ottawa focuses on scaling up most promising firms with new concierge service. The Logic. https://thelogic.co/news/ottawa-focuses-on-scaling-up-most-promising-firms-with-new-concierge-service/ ; Ministry of Citizens' Services. (n.d.). Procurement Concierge Program—Province of British Columbia. Government of British Columbia; Province of British Columbia. Retrieved October 7, 2022, from https://www2.gov.bc.ca/gov/content/bc-procurement-resources/policy-and-strategies/strategies-and-initiatives/procurement-concierge-program

[98] National Cyber Security Centre. (2021). *White paper: The future of NCSC Technology Assurance*. National Cyber Security Centre. https://www.ncsc.gov.uk/collection/technology-assurance/future-technology-assurance

[99] Ibid.

[100] *The current state of technology assurance*. (2021, September 24). NCSC. https://www.ncsc.gov.uk/collection/technology-assurance/future-technology-assurance

[101] Ensor, C. (2021, September 24). *The future of Technology Assurance in the UK*. NCSC. https://www.ncsc.gov.uk/collection/technology-assurance/future-technology-assurance

[102] Donaldson, S., Crozier, D., Matorell, S., McLaren, I., Douglas, J., & Shah, J. N. (2022). UK Cyber Security Sectoral Analysis 2022. Department for Digital, Culture, Media and Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1055565/Cyber_Sectoral_Analysis_2022_Report_V2.1.pdf

[103] Ibid.

[104] Expert Panel on Intellectual Property. (2020). Intellectual Property in Ontario's Innovation Ecosystem. Ministry of Colleges and Universities. https://www.ontario.ca/document/report-intellectual-property-in-ontarios-innovation-ecosystem

[105] Schiavo, N., & Kamat, A. (2022). *Modernizing SR&ED to Support Canada's "Scale-Up" Companies*. Council of Canadian Innovators. https://8440337.fs1.hubspotusercontent-na1.net/hubfs/8440337/Policy%20Brief%20-%20SR%26ED%20September%202022-1.pdf

[106] Ibid.

[107] HHRG-116-IG10: *The Unseen Conflict: Strategic Technology Competition: Hearings before the Strategic Technology and Advanced Research Subcommittee of the House Permanent Select Committee on Intelligence*. Testimony of Mr. Christopher Darby. (2020). https://www.congress.gov/116/meeting/house/110489/witnesses/HHRG-116-IG10-Bio-DarbyC-20200212.pdf

[108] *Tutorial 1: What Is The Purpose Of The Sbir & Sttr Programs?* (n.d.). SBIR. Retrieved October 4, 2022, from https://www.sbir.gov/tutorials/program-basics/tutorial-1

[109] Schiavo, N., & Kamat, A. (2022). *Modernizing SR&ED to Support Canada's "Scale-Up" Companies*. Council of Canadian Innovators. https://8440337.fs1.hubspotusercontent-na1.net/hubfs/8440337/Policy%20Brief%20-%20SR%26ED%20September%202022-1.pdf

[110] Bahr-Gedalia, U. & Dickman, M. (2021, September). Can Canada be a global cybersecurity leader? Innovating Canada. https://www.innovatingcanada.ca/business-and-economy/can-canada-be-a-global-cybersecurity-leader/.

[111] Deloitte & Toronto Financial Services Alliance. (2018). *The changing faces of cybersecurity: Closing the cyber risk gap*. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF

[112] Ibid.

[113] Accelerated Cybersecurity Training Program – Overview: CyberSecure Catalyst. (n.d.). CyberSecure Catalyst. Retrieved October 7, 2022, from https://www.cybersecurecatalyst.ca/actp-overview

[114] *CVCA State of Diversity and Inclusion 2019*. (2019). Canadian Venture Capital and Private Equity Association. https://www.cvca.ca/files/reports/2019-state-of-diversity/CVCA-State-of-Diversity-and-Inclusion-2019.pdf