



State of Canada's Cybersecurity Industry

Fall 2022



Objective: Develop relevant, quality and timely strategic information on Canadian production of cybersecurity goods and services to brief policy and industry decision makers

- **Canada is the first OECD* country to conduct an in-depth Government statistical agency survey on cybersecurity industry capabilities from the supplier perspective**
 - Complementary to Statistics Canada's '*Survey of Cybersecurity and Cybercrime*' (user perspective)

- **Supported by a multi-year collaborative analytics agreement with industry associations**



- **This analysis presents a statistical overview of Canadian cybersecurity industry activities in 2020, based on the most recently available data**
- **As such, these findings provide insights into the state of Canada's cybersecurity industry during the first year of the COVID-19 pandemic**
- **The next iteration of the biennial survey will measure 2022 industrial activities**
 - Publication of the basic 2022 data by Statistics Canada is scheduled for early 2024

Survey Refinement & Preparations (May 2020 – February 2021):

- Consultation with industry, subject matter experts, defence and public security organizations, and policy makers on the research framework and updating the targeted population and questionnaire

Data Development (March 2021 – January 2022):

- Innovation, Science and Economic Development Canada (ISED) sponsored Statistics Canada biennial survey measuring 2020 activities (first year of COVID-19) with completion a legal requirement under the Statistics Act
 - Previous data collection efforts measured 2018 with those findings summarised under a previous report
 - The next round of data collection will measure 2022 industrial activities
- Data validation and firm-level imputation based on administrative and other data

Data Analysis (May 2022 – September 2022):

- Economic impact estimation based on a methodology informed by experts at the OECD and Statistics Canada
- Data analytics and report structure development

Core Areas of Research and Analysis



Comparative Analysis, 2018-2020



Regional Areas of Strength



Economic Impact



Skills/STEM



Size of Firm Footprint



Innovation



Ownership Type



Exports

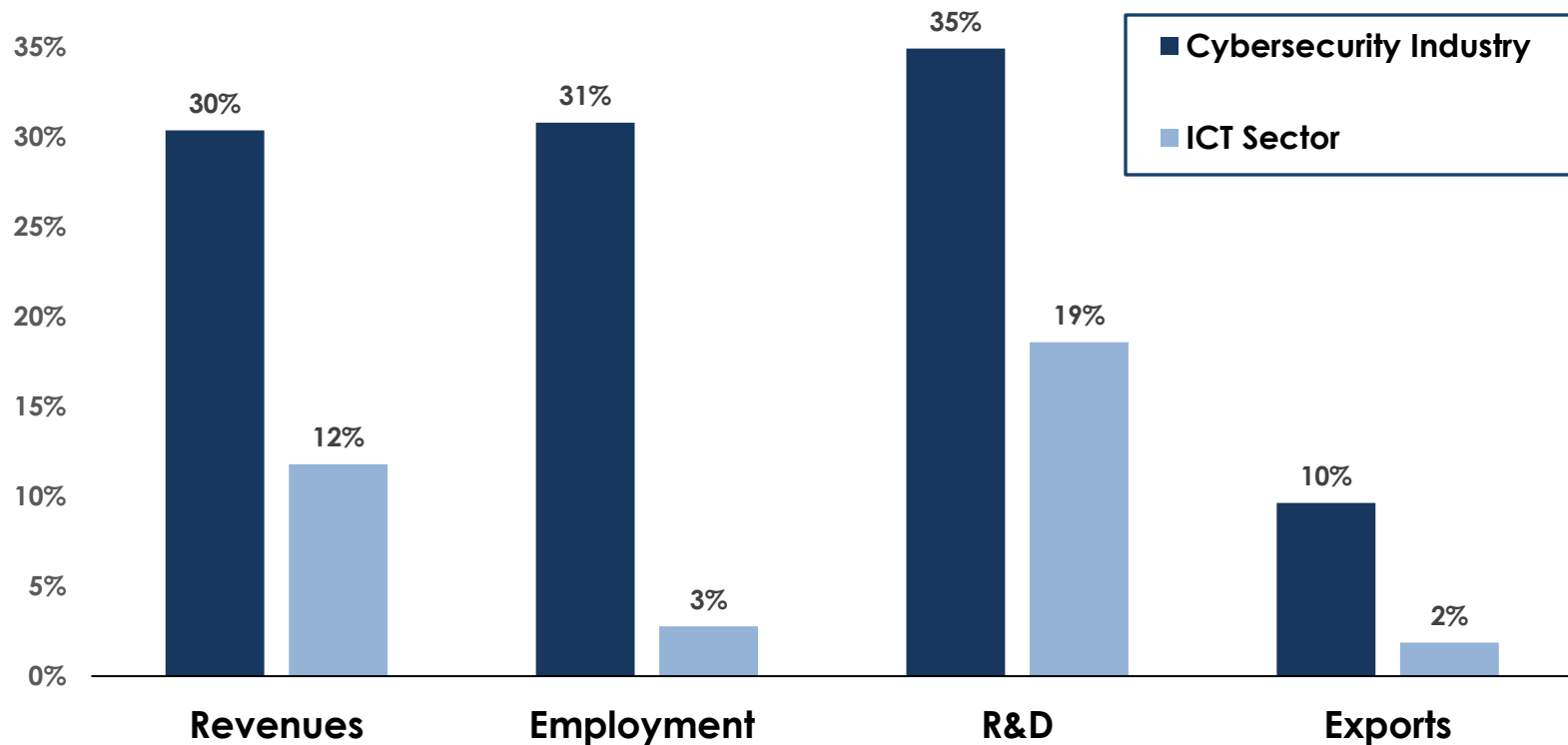


Activities by Type



Canada's cybersecurity industry outperformed the broader ICT sector across industrial indicators between 2018 and 2020*

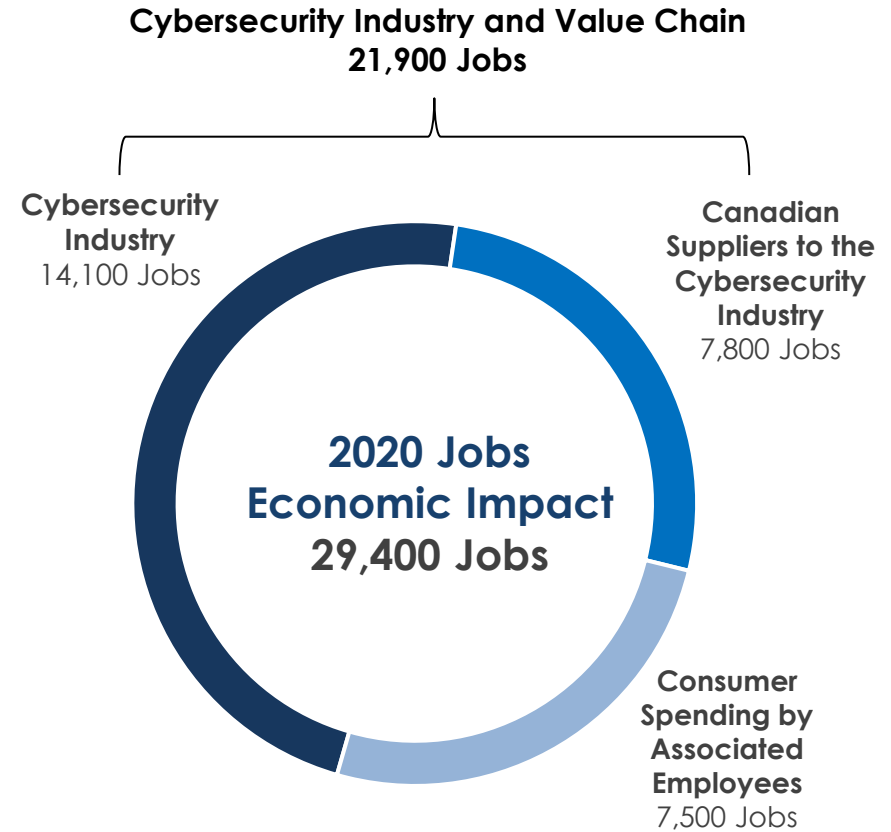
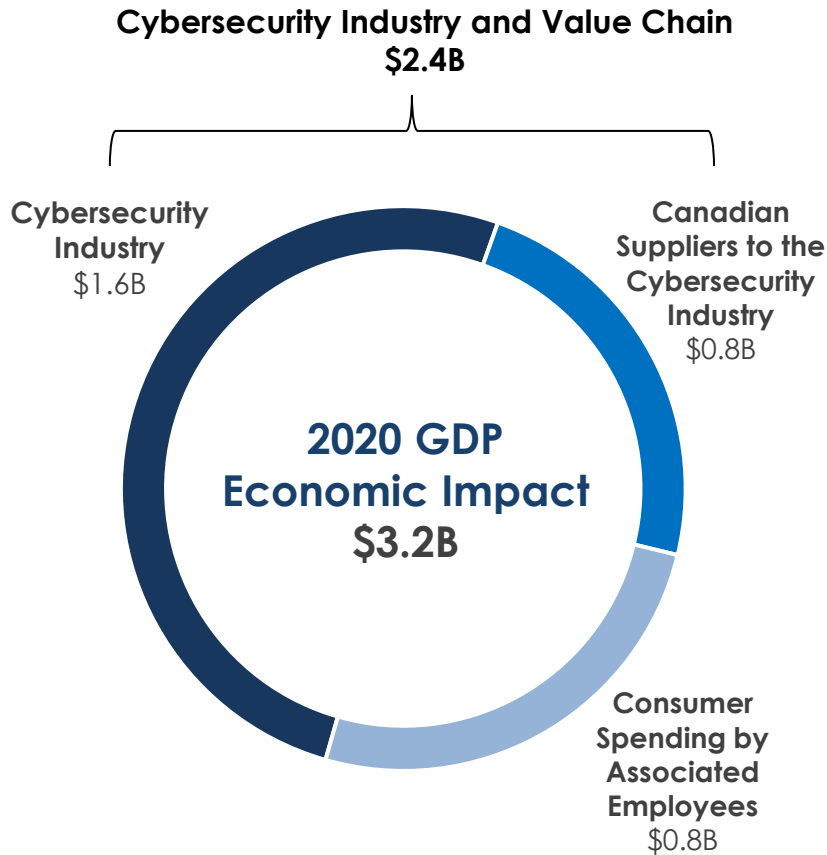
Performance of Key Variables
Canadian Cybersecurity Industry vs. Broader ICT Sector
% Change, 2018-2020*



* Notes: Financial values are in nominal terms and are not adjusted for inflation, and R&D spending relates to businesses' in-house R&D. ICT stands for: Information and Communications Technologies. See annex for associated data tables and definitions of the ICT Sector
Source: Statistics Canada's Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018, 2020), 2020 survey released in 2022; and ISED's "[2021 Canadian ICT Sector Profile](#)" released in 2022, and related ICT profile data from online and custom Statistics Canada data tables



Canada's cybersecurity industry contributed over \$3.2B in GDP and 29,000 jobs across the Canadian economy in 2020*

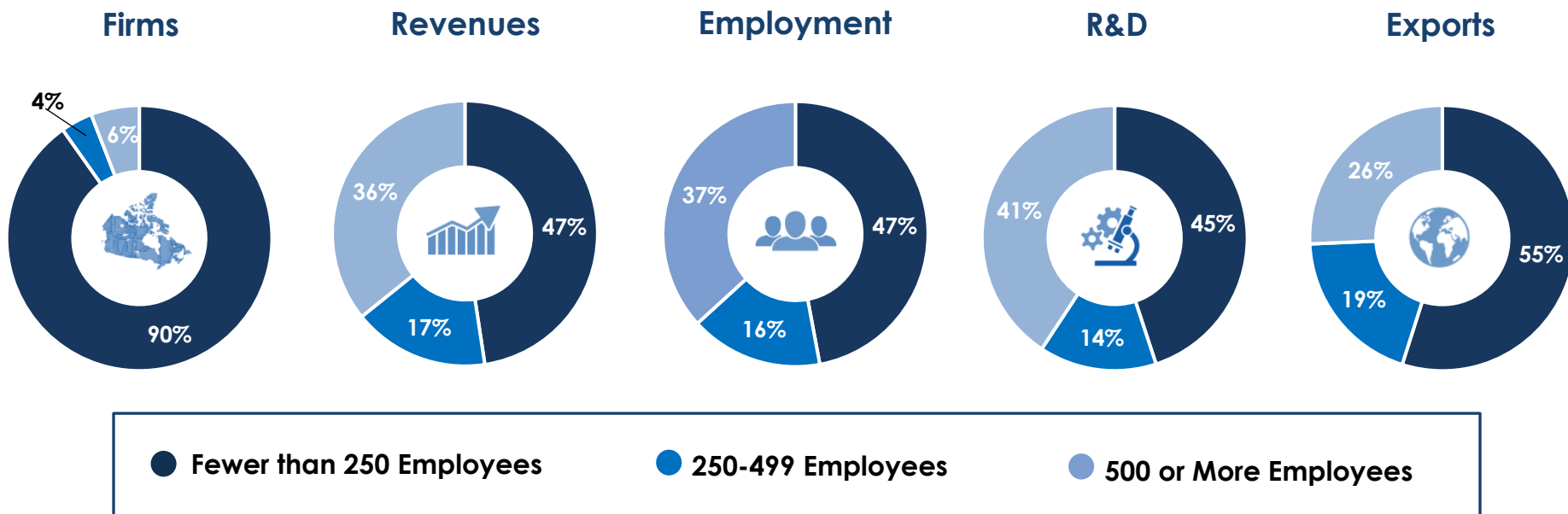


- Total economic activity supported by the Canadian cybersecurity industry increased by over \$860M in GDP and 6,900 jobs between 2018 and 2020

* See annex for associated data tables
Source: Statistics Canada's Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018, 2020), 2020 survey released in 2022; ISED economic modelling based on Statistics Canada's latest input-output multipliers (2016 and 2018), and the specific economic impact multipliers most relevant to the survey's scope of cybersecurity goods and services



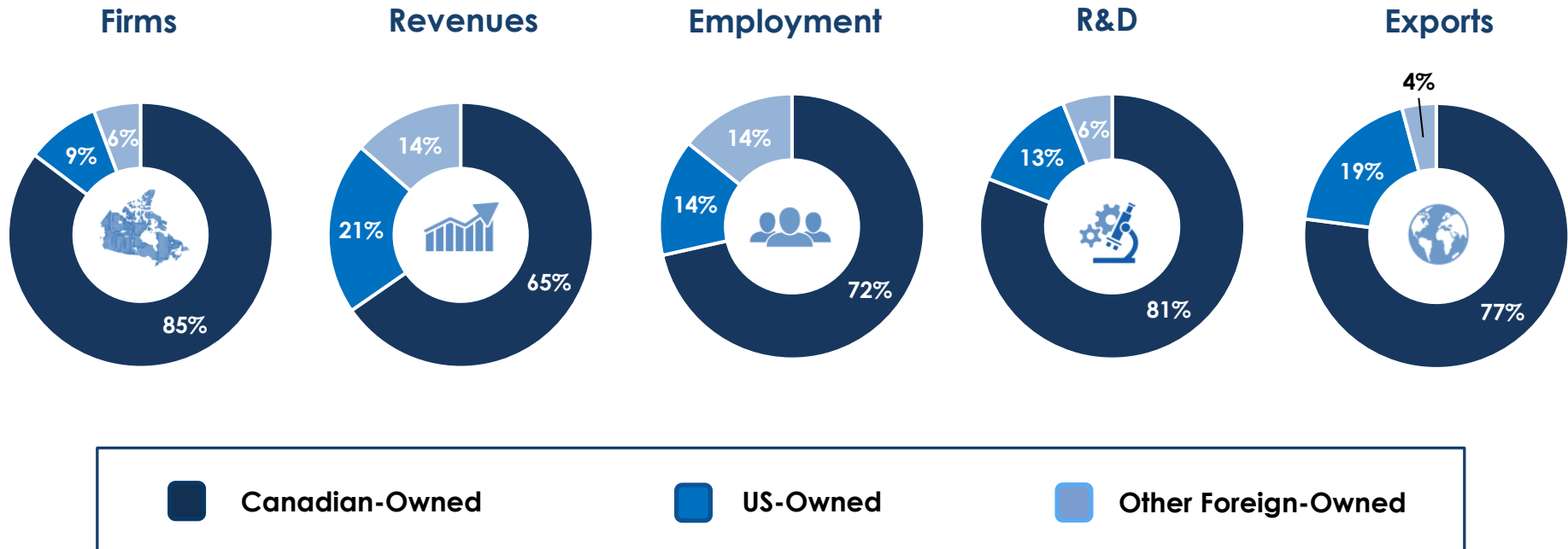
Firms with fewer than 250 employees accounted for 90% of firms and 45% or more of revenues, employees, R&D and exports



- Firms with 250-499 employees accounted for under 20% of revenues, employment, R&D, and exports
- Firms with 500 plus employees accounted for over 35% of revenues, employment and R&D, and as a group were the most R&D-oriented but least export-oriented



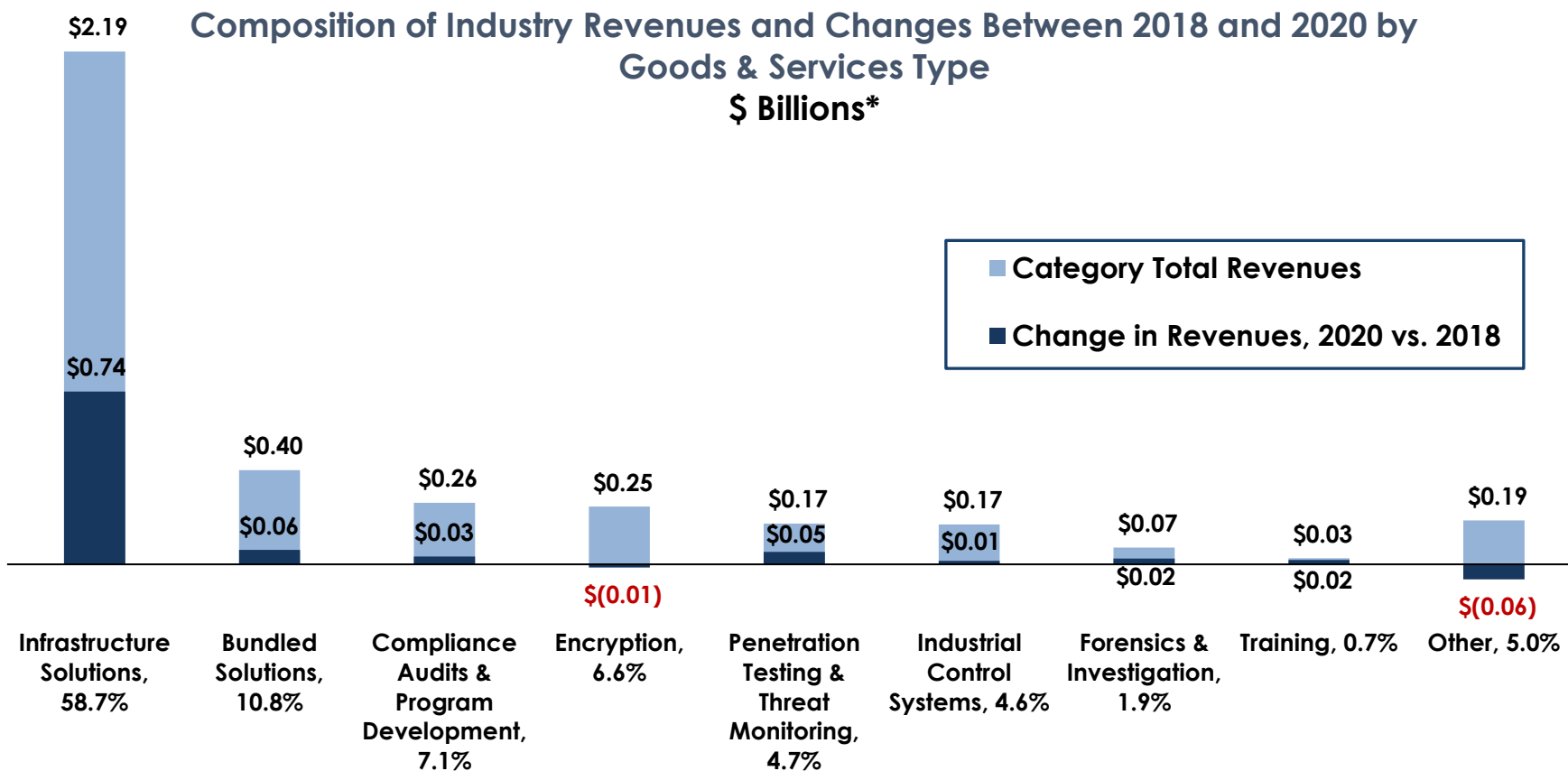
Over 490 firms earned more than \$3.7B in cybersecurity revenues, of which close to 85% were Canadian-owned in 2020*



- **Canadian-owned firms led in terms of revenues, employment, R&D and exports**
 - The operations of foreign owned-firms were also notable and engaged in exports and R&D



Total revenues and growth were led by cyber infrastructure solutions for the ongoing protection of networks and data in 2020



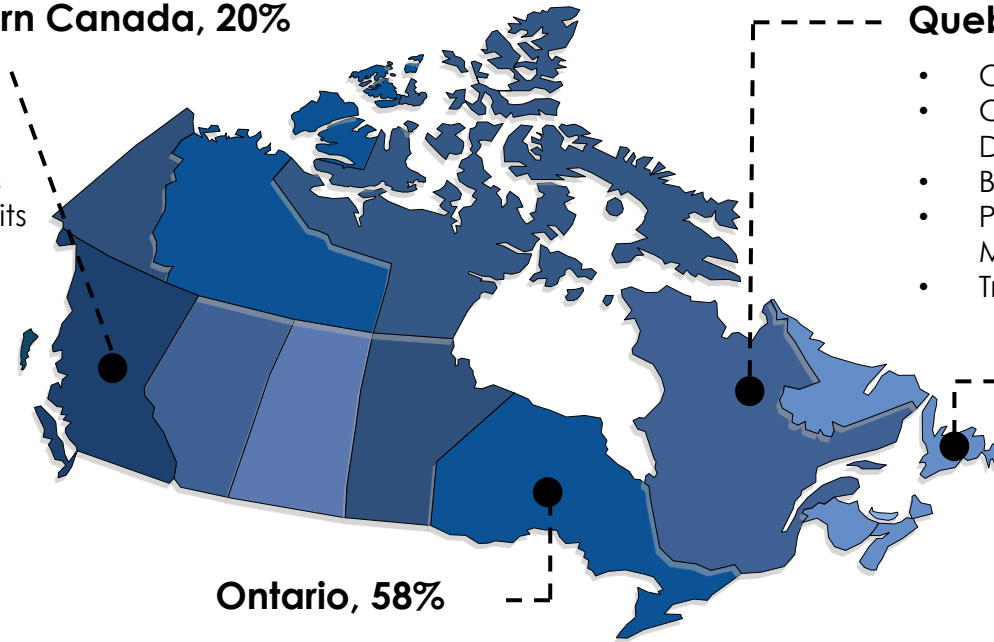
- **Beyond cyber infrastructure solutions, remaining industry revenues were fragmented across the provision of various other goods and services**

Each region had specific areas of strength in 2020*

Canadian Cybersecurity Industry Employment Regional Breakdown** with Top Regional Specializations 2020

Western & Northern Canada, 20%

- Cybersecurity Infrastructure Solutions
- Bundled Solutions
- Compliance Audits & Program Development
- Encryption
- Industrial Control Systems



Quebec, 15%

- Cybersecurity Infrastructure Solutions
- Compliance Audits & Program Development
- Bundled Solutions
- Penetration Testing & Threat Monitoring
- Training

Atlantic Canada, 7%

- Industrial Control Systems
- Bundled Solutions
- Cybersecurity Infrastructure Solutions
- Compliance Audits & Program Development
- Training

Ontario, 58%

- Cybersecurity Infrastructure Solutions
- Bundled Solutions
- Compliance Audits & Program Development
- Penetration Testing & Threat Monitoring
- Encryption

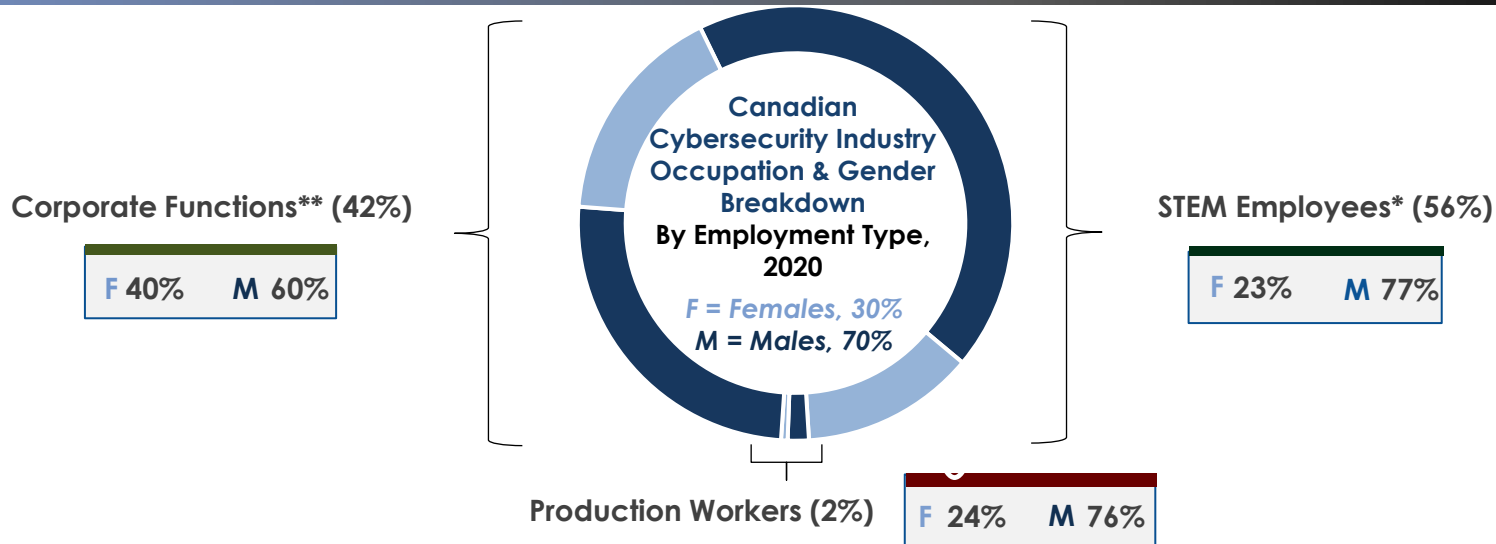
* See annex for the associated data table with the ranking of all categories per region, and for the full official titles of the cybersecurity goods and services categories

** Shares of employment by region are based on businesses that specified their regional employment breakdown and reflect the cybersecurity industry's own 14.1K in total employees. The rankings of top 5 activities per region as presented here exclude a survey category which covered a mix of other (unspecified) cybersecurity goods and services

Source: Statistics Canada's Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2020), 2022



STEM* occupations led employment in the cybersecurity industry in 2020



- **STEM occupations' share of cybersecurity industry employment was similar to that of the ICT industry*** and close to 6X that of Canada's overall industrial base**

Female Employees' Share of Occupation Types		
Occupation Type	Canada's Cybersecurity Industry	Canada's ICT Sector****
Corporate Functions	40%	44%
STEM	23%	21%
Production Workers	24%	16%
TOTAL	30%	29%

* Under the survey, Science, Technology, Engineering & Mathematics (STEM) occupations include engineers, scientists and/or researchers, and technicians and technologists. See annex for associated data tables. STEM occupations' shares of category-level employment are also available, and are provided in the annex for insights into differences in the relative STEM orientation of specific cybersecurity activities' workforces

** Includes occupations in: management, administration, marketing, and all other employees

*** See annex for ICT Industry definitions and for associated data tables

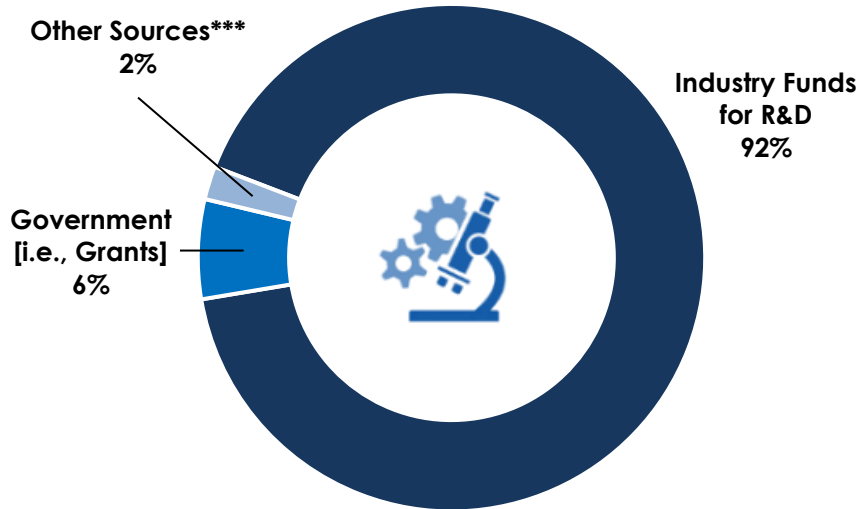
**** Estimates based on data where breakdowns of activities by occupation and gender type were more fully specified for NAICS industries under the ICT Sector

Source: Statistics Canada's Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2020), 2022; and Statistics Canada custom tabulations based on the Labour Force Survey (2020), 2022

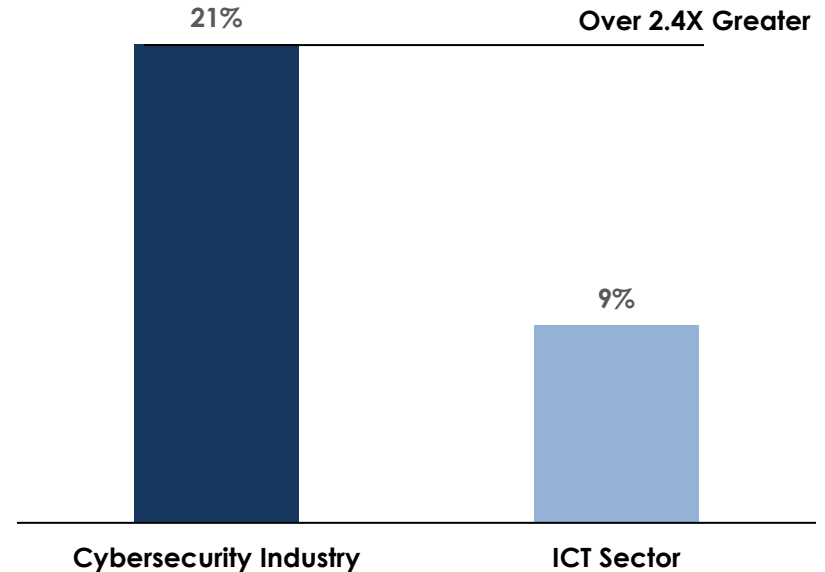


The cybersecurity industry's R&D intensity* was close to 2.5X greater than the Canadian ICT industry's** average in 2020

Canadian Cybersecurity Industry R&D Breakdown by Source of Funds 2020



R&D Intensity Cybersecurity vs. ICT Industry 2020



- **Over \$347M of R&D was performed by the industry, led by experimental development in 2020**
 - More than 90% was funded by industry—led by funds from parent companies, affiliates & subsidiaries of the cybersecurity industry R&D performers; followed by the internal funds of the R&D performers****

* Industry-level R&D intensity is measured as the ratio of R&D performed by a given industry or sector relative to its own GDP. At the level of individual cybersecurity goods & services categories, R&D to GDP ratios are not available, but ratios of category-level R&D to sales are available, and are provided in the annex for insights into differences in relative R&D orientation across specific cybersecurity activities

** See annex for ICT Industry definitions, and for associated data tables

*** Other sources may include universities, foreign governments, individuals, etc.

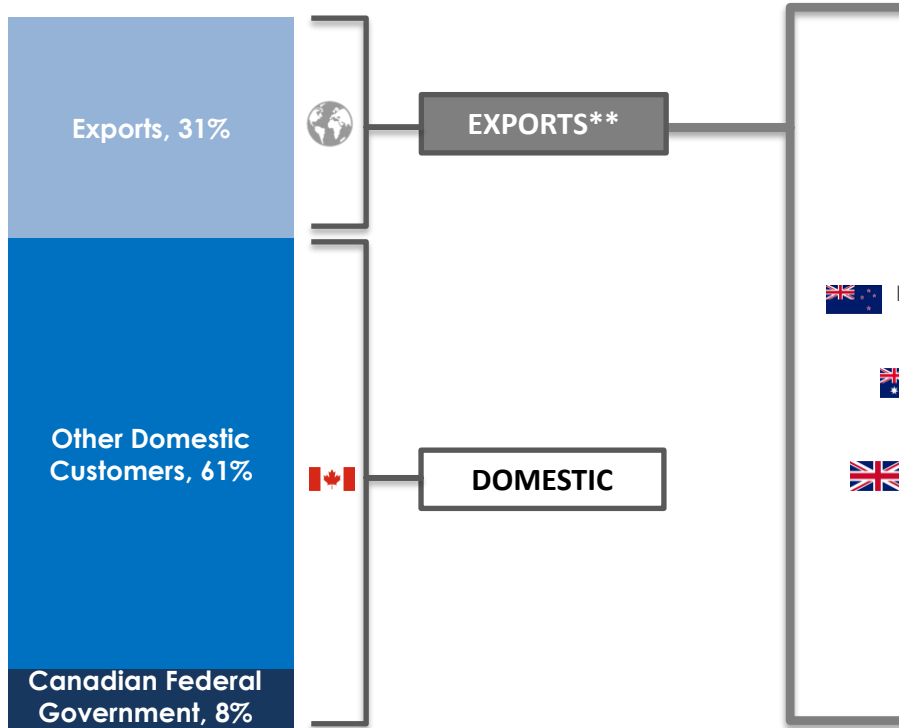
**** While only 6% of total R&D was government funded, 'Cybersecurity Training' R&D was an exception, with 40% < X ≤ 50% of its R&D government funded

Source: Statistics Canada's Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2020), 2022; ISED estimates of cybersecurity industry GDP; ISED's "2021 Canadian ICT Sector Profile", released in 2022 and related ICT profile data from online and custom Statistics Canada data tables; and Statistics Canada Table 36-10-0106-01 for GDP price indexes

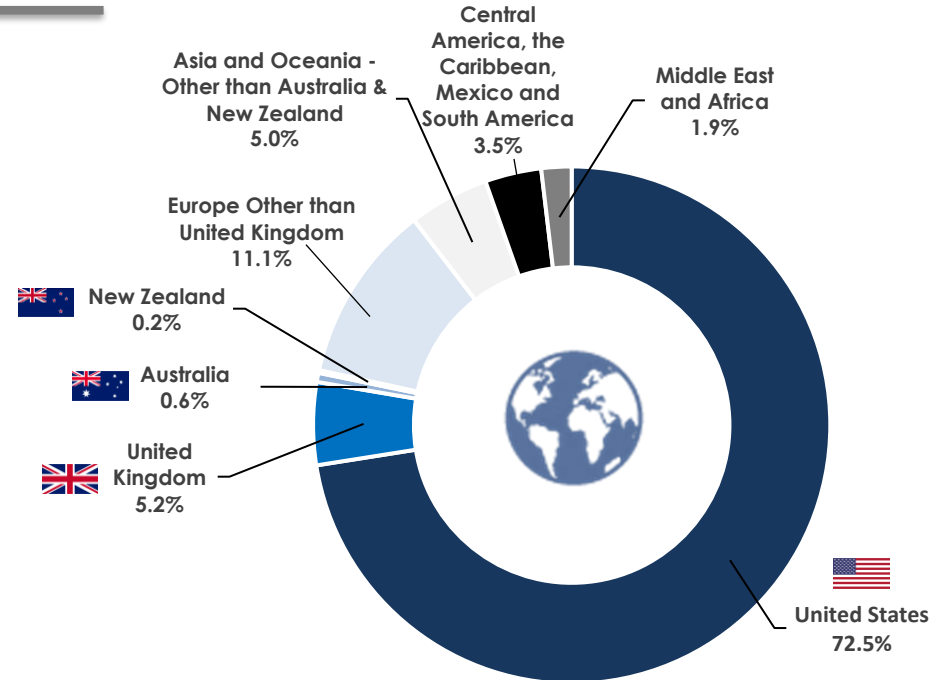


Over \$1.15B in exports, with close to 80% accounted for by Canada's Five Eyes partners*

Cybersecurity Industry Domestic Revenues vs. Exports 2020



Cybersecurity Industry Exports Breakdown by Region 2020



- Export intensity was close to 2.5X higher than the ICT industry average in 2020***

* The Five Eyes partner nations include: Australia, Canada, New Zealand, the United Kingdom, and the United States

** Ratios of category-level exports to sales are also available and are provided in the annex for insights into differences in the relative export orientation of specific cybersecurity activities

*** See annex for ICT Industry definitions and associated data tables

Source: Statistics Canada's Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2020), 2022; and ISED's "2021 Canadian ICT Sector Profile", released in 2022, and related ICT data from online and custom Statistics Canada data tables



In 2020, Canada's cybersecurity industry:

- **Outperformed the broader ICT sector across industrial indicators since 2018**
- **Was led by Canadian-owned firms, and by firms with fewer than 250 employees**
- **Contributed over 29,000 jobs to the Canadian economy**
 - **An increase of close to 6,900 jobs between 2018 and 2020**
- **Was national in scope, with regional specializations**
- **Was STEM-oriented and R&D-intensive, with over \$1.15B of exports**



Annexes



Annex 1: Economic Impact Methodology Principles

- **Foundation data is from the latest (2020) Statistics Canada “*Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey*” released in 2022**
- **ISED economic modelling is based on Statistics Canada’s latest Input-Output multipliers (2018) and closest related specific economic impact multipliers that relate to cybersecurity activities**
 - Cybersecurity activity has been linked to the latest (2018) and most relevant specific economic impact multipliers per cybersecurity goods and services category
 - GDP impact is reported cumulatively and on a yearly average basis
 - Job impact is reported on an annual average basis and measured in terms of full-time equivalent employment (FTE)
 - Jobs cannot be additive as they are maintained for an extended period after creation
 - Total economic impact of the cybersecurity industry includes the activity that occurs within the Canadian cybersecurity industry, plus activity among Canadian suppliers to the Canadian cybersecurity industry, as well as consumer spending by associated employees across the Canadian economy
 - Economic impact estimates are reported at the national level and cannot be broken down at the regional level



Annex 2: NAICS Comprising the ICT Sector

NAICS Code	NAICS Code Title
3341	Computer and Peripheral Equipment Manufacturing
3342	Communications Equipment Manufacturing
3343	Audio and Video Equipment Manufacturing
3344	Semiconductor and Other Electronic Component Manufacturing
3346	Manufacturing and Reproducing Magnetic and Optical Media
4173	Total ICT Wholesaling
5112	Software Publishers
517	Communications Services
5182	Data Processing, Hosting and Related Services
5415	Computer Systems Design and Related Services
8112	Electronic and Precision Equipment Repair and Maintenance



Annex 3: Data Tables

Table I: Cybersecurity and ICT Sector Industry Revenues, Employment, R&D and Exports, % Change—2018 to 2020*

	Cybersecurity	ICT Sector
Revenues	30%	12%
Employment	31%	3%
R&D	35%	19%
Exports	10%	2%

Table II: Economic Impact**

GDP Economic Impact (\$B)				
Cybersecurity Industry	Suppliers to Cybersecurity Industry	Cybersecurity Industry and Value Chain	Consumer Spending by Associated Employees	Cumulative Total GDP
\$ 1.636	\$ 0.749	\$ 2.385	\$ 0.823	\$ 3.208

Job Economic Impact				
Cybersecurity Industry	Suppliers to Cybersecurity Industry	Cybersecurity Industry and Value Chain	Consumer Spending by Associated Employees	Total Annual Average Jobs
14,107	7,796	21,903	7,544	29,447

* Note: Financial values are in nominal terms and are not adjusted for inflation, and R&D spending relates to businesses' in-house R&D. ICT stands for "Information and Communications Technologies"

** ISED's economic modelling is based on Statistics Canada's latest input-output multipliers (2016 and 2018), and the specific economic impact multipliers most relevant to the survey's scope of cybersecurity goods and services

Source: Statistics Canada's Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018, 2020), 2020 survey released in 2022; and ISED's "[2021 Canadian ICT Sector Profile](#)" released in 2022, and related ICT profile data from online and custom Statistics Canada data tables



Annex 3: Data Tables (cont.)

Table III: Firm Size Breakdown

Size Breakdown	Share of Total Cybersecurity Industry Enterprise Counts	Share of Total Cybersecurity Industry Revenues	Share of Total Cybersecurity Industry Employment	Share of Total Cybersecurity Industry R&D	Share of Total Cybersecurity Industry Exports
Enterprises with fewer than 250 employees	90.2%	47.6%	47.1%	44.9%	54.9%
Enterprises with between 250 and 499 employees	3.9%	16.6%	16.2%	14.3%	19.4%
Enterprises with 500 or more employees	5.9%	35.8%	36.7%	40.8%	25.7%
Total Enterprises	100%	100%	100%	100%	100%

	Number of Cybersecurity Industry Enterprises	Counts of Enterprises Performing R&D	Counts of Enterprises Not Performing R&D	Counts of Enterprises that Didn't Specify if They Performed R&D
Enterprises with fewer than 250 employees	442	176	254	12
Enterprises with between 250 and 499 employees	19	10	9	0
Enterprises with 500 or more employees	29	16	8	5
Total	490	202	271	17

Table IV: Key Industrial Indicators by Country of Ownership*

Country of Ownership Breakdown	Share of Total Cybersecurity Industry Enterprise Counts	Share of Total Cybersecurity Industry Revenues	Share of Total Cybersecurity Industry Employment	Share of Total Cybersecurity Industry R&D	Share of Total Cybersecurity Industry Exports
Canadian-Owned	85.3%	65.3%	71.6%	80.9%	77.1%
US-Owned	9.0%	21.2%	14.2%	13.0%	18.7%
Other Foreign-Owned	5.7%	13.5%	14.2%	6.1%	4.2%
Total Enterprises	100%	100%	100%	100%	100%

* Ownership status based on location of parent companies
 Source: Statistics Canada's Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2020), 2022



Annex 3: Data Tables (cont.)

Table V: Cybersecurity Revenues by Goods & Services Types*

	Category Total Revenues, \$B	Change in Revenues, \$B, 2020 vs. 2018
Infrastructure Solutions, 58.7%	\$ 2.19	\$ 0.74
Bundled Solutions, 10.8%	\$ 0.40	\$ 0.06
Compliance Audits & Program Development, 7.1%	\$ 0.26	\$ 0.03
Encryption, 6.6%	\$ 0.25	-\$ 0.01
Penetration Testing & Threat Monitoring, 4.7%	\$ 0.17	\$ 0.05
Industrial Control Systems, 4.6%	\$ 0.17	\$ 0.01
Forensics & Investigation, 1.9%	\$ 0.07	\$ 0.02
Training, 0.7%	\$ 0.03	\$ 0.02
Other, 5.0%	\$ 0.19	-\$ 0.06

* Revenues are not adjusted for inflation.

Source: Statistics Canada's Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2020), 2022



Annex 3: Data Tables (cont.)

Table VI: Regional Ranking of Activities*

Rank by Employment Within Region	Atlantic Canada
1	Industrial Control Systems
2	Bundled Solutions
3	Cybersecurity Infrastructure Solutions
4	Compliance Audits & Program Development
5	Training
6	Penetration Testing & Threat Monitoring
7	Forensics & Investigation
8	Encryption
+	Other

+ If the 'Other Cybersecurity Goods & Services' category is included with the more specific categories, it ranks 7th.

Rank by Employment Within Region	Quebec
1	Cybersecurity Infrastructure Solutions
2	Compliance Audits & Program Development
3	Bundled Solutions
4	Penetration Testing & Threat Monitoring
5	Training
6	Encryption
7	Industrial Control Systems
8	Forensics & Investigation
+	Other

+ If the 'Other Cybersecurity Goods & Services' category is included with the more specific categories, it ranks 5th.

* Shares of employment by region are based on businesses that specified their regional employment breakdown and reflect the cybersecurity industry's own 14.1K in total employees
Source: Statistics Canada's Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2020), 2022



Annex 3: Data Tables (cont.)

Table VI: Regional Ranking of Activities (cont.)*

Rank by Employment Within Region	Ontario
1	Cybersecurity Infrastructure Solutions
2	Bundled Solutions
3	Compliance Audits & Program Development
4	Penetration Testing & Threat Monitoring
5	Encryption
6	Forensics & Investigation
7	Industrial Control Systems
8	Training
+	Other

+ If the 'Other Cybersecurity Goods & Services' category is included with the more specific categories, it ranks 6th.

Rank by Employment Within Region	Western and Northern Canada
1	Cybersecurity Infrastructure Solutions
2	Bundled Solutions
3	Compliance Audits & Program Development
4	Encryption
5	Industrial Control Systems
6	Penetration Testing & Threat Monitoring
7	Forensics & Investigation
8	Training
+	Other

+ If the 'Other Cybersecurity Goods & Services' category is included with the more specific categories, it ranks 2nd.

* Shares of employment by region are based on businesses that specified their regional employment breakdown and reflect the cybersecurity industry's own 14.1K in total employees
Source: Statistics Canada's Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2020), 2022



Annex 3: Data Tables (cont.)

Table VII: Regional Distribution of Employment

Regional Breakdown	Western and Northern Canada	Ontario	Quebec	Atlantic Canada
Distribution of Employment in the Cybersecurity Industry	20%	58%	15%	7%

Table VIII: Occupation and Gender Breakdown

Occupation Breakdown	Share of Employment by Occupation	Gender Breakdown	Share of Occupation Employees by Gender
STEM*	56%	Male	77%
		Female	23%
Production Workers	2%	Male	76%
		Female	24%
Corporate Functions**	42%	Male	60%
		Female	40%
All Employees	100%	Male	70%
		Female	30%

Female Employees' Share of Occupation Types		
Occupation Type	Canada's Cybersecurity Industry	Canada's ICT Sector***
Corporate Functions	40%	44%
STEM	23%	21%
Production Workers	24%	16%
TOTAL	30%	29%

* Under the survey, Science, Technology, Engineering & Mathematics (STEM) occupations include engineers, scientists and/or researchers, and technicians and technologists. See annex for associated data tables

** Includes occupations in: management, administration, marketing, and all other employees

*** Estimates based on data where breakdowns of activities by occupation and gender type were more fully specified for NAICS industries under the ICT Sector

Source: Statistics Canada's Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2020), 2022; and Statistics Canada custom tabulations based on the Labour Force Survey (2020), 2022



Annex 3: Data Tables (cont.)

Table IX: STEM Share of Category Level Employment*

	Category Revenues	Ranking, from Highest to Lowest Share of Cybersecurity Industry Employment	Share of a Category's Employees in STEM Occupations	Ranking, from Highest to Lowest STEM Share of a Category's Employment
Industrial control systems (ICS); supervisory control and data acquisition (SCADA) and operation technology (OT) related cybersecurity	\$ 170,577,097	4	60% < X ≤ 70% Value of Uncertain Statistical Reliability	1 Value of Uncertain Statistical Reliability
Encryption	\$ 246,812,300	7	60% < X ≤ 70%	2
Cybersecurity solutions based on a single package of services, software and/or hardware—and involving elements of several of the preceding cybersecurity categories.	\$ 402,764,728	2	60% < X ≤ 70%	3
Penetration testing and associated vulnerability & threat assessments, cyberspace threat monitoring, detection, intelligence services, and active cyber defence measures	\$ 174,023,686	6	60% < X ≤ 70%	4
Compliance audits & program development, strategy development, and related risk management and consulting services	\$ 263,543,386	3	50% < X ≤ 60%	5
Cybersecurity infrastructure services and solutions for the ongoing protection of networks and data	\$ 2,192,703,687	1	50% < X ≤ 60%	6
Forensics and the investigation of, and response to, cyber-attacks or other cyber incidents and intrusions	\$ 72,238,812	8	50% < X ≤ 60%	7
Other cybersecurity related goods & services	\$ 187,580,158	5	40% < X ≤ 50%	8
Cybersecurity training	\$ 26,443,076	9	30% < X ≤ 40%	9

* Based on the responses of businesses who specified the breakdown of their employees by occupation type
Source: Statistics Canada's Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2020), 2022 custom tables



Annex 3: Data Tables (cont.)

Table X: R&D Funding, and Intensity Comparison with ICT Sector

Sources of Funding for R&D	Share of R&D Breakdown
Industry Funds for R&D	92%
Government [i.e., Grants]*	6%
Other Sources**	2%

	R&D Intensity Relative to GDP***
Cybersecurity Industry	21%
ICT Sector	9%

* While only 6% of total in-house R&D was government funded, 'Cybersecurity Training' R&D was an exception, with 40% < X ≤ 50% of its R&D government funded

** Other sources may include universities, foreign governments, individuals, etc.

*** Industry-level R&D intensity is measured as the ratio of R&D performed by a given industry or sector relative to its own GDP

Source: Statistics Canada's Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2020), 2022; ISED estimates of cybersecurity industry GDP; ISED's "2021 Canadian ICT Sector Profile", released in 2022 and related ICT profile data from online and custom Statistics Canada data tables; and Statistics Canada Table 36-10-0106-01 for GDP price indexes



Annex 3: Data Tables (cont.)

Table XI: Cybersecurity Goods & Services Categories' R&D to Revenues Ratios*

	Category Revenues	Category R&D Relative Revenues	Ranking, from Highest to Lowest R&D to Revenue Ratio
Forensics & Investigation	\$ 72,238,812	$X > 15\%$	1
Training	\$ 26,443,076	$9\% < X \leq 12\%$	2
Infrastructure Solutions	\$ 2,192,703,687	$9\% < X \leq 12\%$	3
Bundled Solutions	\$ 402,764,728	$9\% < X \leq 12\%$	4
Other	\$ 187,580,158	$9\% < X \leq 12\%$	5
Encryption	\$ 246,812,300	$6\% < X \leq 9\%$	6
Penetration Testing & Threat Monitoring	\$ 174,023,686	$3\% < X \leq 6\%$	7
Industrial Control Systems	\$ 170,577,097	$3\% < X \leq 6\%$	8
Compliance Audits & Program Development	\$ 263,543,386	$0\% \leq X \leq 3\%$	9

* At the level of individual cybersecurity goods & services categories, R&D to GDP ratios are not available, but ratios of category-level R&D to sales are available and are presented here for insights into differences in relative R&D orientation across specific cybersecurity activities

Source: Statistics Canada's Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2020), 2022 custom tables



Annex 3: Data Tables (cont.)

Table XII: Domestic and Foreign Market Breakdown

Cybersecurity Domestic Revenues	69%	Cybersecurity Export Revenues	31%
Domestic Revenues by Customer Type		Export Revenues by Destination	
•Canadian Federal Government	12.0%	•United States	72.5%
•Other Canadian Customers	88.0%	•United Kingdom (UK)	5.2%
		•Australia	0.6%
		•New Zealand	0.2%
		•Canada's "Five Eyes" Allies	78.5%
		•Europe Other than UK	11.1%
		•Asia & Oceania - Other than Australia & New Zealand	5.0%
		•Central America, the Caribbean, Mexico & South America	3.5%
		•Middle East and Africa	1.9%
Cybersecurity Domestic Revenues Total	100%	Cybersecurity Export Revenues Total	100%



Annex 3: Data Tables (cont.)

Table XIII: Cybersecurity Goods & Services Categories' Exports to Revenues Ratios

	Category Revenues	Category Exports Relative Revenues	Ranking, from Highest to Lowest R&D to Revenue Ratio
Forensics & Investigation	\$ 72,238,812	60% < X ≤ 80%	1
Other	\$ 187,580,158	60% < X ≤ 80%	2
Training	\$ 26,443,076	40% < X ≤ 60%	3
Infrastructure Solutions	\$ 2,192,703,687	20% < X ≤ 40%	4
Bundled Solutions	\$ 402,764,728	20% < X ≤ 40%	5
Penetration Testing & Threat Monitoring	\$ 174,023,686	0% ≤ X ≤ 20%	6
Encryption	\$ 246,812,300	0% ≤ X ≤ 20%	7
Compliance Audits & Program Development	\$ 263,543,386	0% ≤ X ≤ 20%	8
Industrial Control Systems	\$ 170,577,097	0% ≤ X ≤ 20%	9



Annex 4: Cybersecurity Industry Goods & Services Category Definitions

Cybersecurity Industry

To be excluded from this survey are:

Sales of goods and services (e.g., hardware, software, consulting services, R&D, hosted cybersecurity services) that were essentially produced, or rendered/provided by facilities and employees located outside of Canada and delivered as is to customers in Canada or abroad.

Therefore, to be excluded are sales relating to any transactions with, arranged or contracted through business entities, intermediaries or representatives in Canada for goods and/or services to essentially be sourced from businesses outside of Canada. Sales relating to distribution, retail, and wholesale activities

Full Official Titles and Definitions of Cybersecurity Goods & Services Categories	Abbreviated Title Versions
<p>Compliance audits & program development, strategy development, and related risk management and consulting services</p> <p>This category includes sales related to both production of goods and/or the provision of services (including research, development, design, engineering, testing & evaluation services), such as relating to:</p> <ul style="list-style-type: none"> • cybersecurity audits / compliance audits • cybersecurity strategy development • cybersecurity compliance program development, • other related risk management and consulting services. 	<p>Compliance Audits & Program Development</p>
<p>Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), and Operation Technology (OT) Related Cyber Security</p> <p>This category includes sales related to both production of goods and/or the provision of services (including research, development, design, engineering, testing & evaluation services), such as relating to:</p> <p>Any cybersecurity related solutions and services intended to protect industrial control systems, SCADA, or operation technology (OT). For example, this may include, but not be limited to, Hardware Security Modules, or Hardware Cryptographic Modules.</p> <p>Excluding protection of enterprise IT networks.</p>	<p>Industrial Control Systems</p>
<p>Encryption</p> <p>This category includes sales related to both production of goods and/or the provision of services (including research, development, design, engineering, testing & evaluation services), such as relating to:</p> <p>Hardware or software based encryption, or services to develop or implement encryption, (this may also include, but not be limited to, activities relating to quantum proof algorithms and encryption).</p> <p>Excluding:</p> <ul style="list-style-type: none"> • integration or resale of commercial encryption is not to be included here • encryption that is primarily included under another goods & services category. 	<p>Encryption</p>



Annex 4: Cybersecurity Industry Goods & Services Category Definitions (cont.)

Full Official Titles and Definitions of Cybersecurity Goods & Services Categories	Abbreviated Title Versions
<p>Cybersecurity infrastructure services and solutions for the ongoing protection of networks and data This category includes sales related to both production of goods and/or the provision of services (including research, development, design, engineering, testing & evaluation services), such as relating to: Services and solutions to establish ongoing protection of networks and data. This includes design, integration, and provision of security infrastructure.</p> <p>Solutions may include or relate to, but not necessarily be limited to:</p> <ul style="list-style-type: none"> • firewalls / next generation firewalls; • intrusion detection and prevention systems (IDS/IPS); • managed Security Service Providers (MSSP); • web application firewalls; • secure email gateways; • end point security, detection & response; • insider threat detection; • identity and access management / control. This can also include systems and software relating to user authentication/recognition based on image, voice and other biometric-based analytic techniques (or various combinations of methods under multi-factor authentication)—for the purposes of ensuring only authorized access to, and use of cyber systems); • application security tools such as Runtime Application Self-Protection (RASP); • services pertaining to security system design, integration, installation; • cybersecurity orchestration and automation; • cloud-based cybersecurity solutions; • other technologies designed to protect against attacks that use cryptanalytic techniques like side-channel analysis of the physical emanations / physical signals (e.g., electromagnetic fields & pulses, power consumption, heat dissipation) of devices during the process of their operation. Examples of attack types include, but are not limited to those involving: timing attacks; power or electromagnetic analysis; and micro-architectural attacks. 	<p style="text-align: center;">Infrastructure Solutions</p>



Annex 4: Cybersecurity Industry Goods & Services Category Definitions (cont.)

Full Official Titles and Definitions of Cybersecurity Goods & Services Categories	Abbreviated Title Versions
<p>Penetration testing and associated vulnerability & threat assessments, cyberspace threat monitoring, detection, intelligence services, and active cyber defence measures</p> <p>This category includes sales related to production of goods and/or the provision of services (which may also include research, development, design, engineering, testing & evaluation services) relating to:</p> <p>Penetration testing; Vulnerability assessments.</p> <p>Activities in the cyber-domain or the cyber space connected to efforts to detect, monitor, analyse, understand, and/or predict cyber threats—such as in order to improve parties' situational awareness and ability to adapt/strengthen their cyber defences accordingly, and to therefore pre-empt or mitigate potential cybersecurity failures.</p> <p>The conduct of more active cyber defense measures like those intended to preserve the ability of a defending party to use/freely operate in cyber-space; and to protect data, networks, network-centric capabilities, infrastructure, and other systems, assets, and property—by searching for, detecting, defeating and/or mitigating a threat's offensive and exploitative cyber capabilities and actions.</p>	<p>Penetration Testing & Threat Monitoring</p>
<p>Forensics and the investigation of, and response to, cyber attacks or other cyber incidents and intrusions</p> <p>This category includes sales related to both production of goods and/or the provision of services (including research, development, design, engineering, testing & evaluation services), such as relating to:</p> <p>Services and software tools involved in identifying, assessing, and responding to cyber-attacks and incidents. Examples may include, but not necessarily be limited to:</p> <ul style="list-style-type: none"> • network forensics; • related hunt services & tools; • fraud analytics; • identification of inside perpetrators; • other incident response services. 	<p>Forensics & Investigation</p>
<p>Cybersecurity training</p> <p>This category includes sales related to both production of goods and/or the provision of services (including research, development, design, engineering, testing & evaluation services), such as relating to:</p> <ul style="list-style-type: none"> • training • workforce development, • educational services or solutions. <p>This includes all levels, from more basic users to advanced practitioners; and spans services, courseware, software, or other delivery mechanisms.</p>	<p>Training</p>



Annex 4: Cybersecurity Industry Goods & Services Category Definitions (cont.)

Full Official Titles and Definitions of Cybersecurity Goods & Services Categories	Abbreviated Title Versions
<p>Cybersecurity Solutions Based on a Single Package of Services, Software and/or Hardware—and Involving Elements of Several of the Preceding Cybersecurity Categories</p> <p>This category includes sales spanning both goods and/or services (including research, development, design, engineering, testing & evaluation services) relating to:</p> <p>Solutions that address customer/client cybersecurity requirements by providing them with a single package of services, software and/or hardware which involves elements relating to more than one of the other preceding cybersecurity goods and services categories and associated functions, tasks.</p> <p>Cybersecurity goods and services sales that can be broken down according to the other individual cybersecurity goods and services categories should be reported under those respective categories, and should NOT be reported under this sales category.</p>	<p>Bundled Solutions</p>
<p>Other cybersecurity related goods & services</p> <p>This category includes sales related to both production of goods and/or the provision of services (including research, development, design, engineering, testing & evaluation services), such as relating to:</p> <p>Other activities that could be considered cybersecurity related in nature, (including those beyond just defensive or passive cybersecurity related activities).</p> <p>For example, privacy and de-identification, or anonymization tools, goods and services related to support of military full spectrum operations not otherwise effectively captured under the preceding sales categories.</p> <p>Excluding sales of goods and services that were essentially produced or rendered/provided by facilities and employees located outside of Canada and delivered as is to customers in Canada or abroad.</p> <p>e.g., sales relating to any transactions with, arranged or contracted through business entities, intermediaries or representatives in Canada for goods and/or services to essentially be sourced from businesses outside of Canada; distribution, retail, and wholesale activities.</p>	<p>Other</p>
<p>** <u>Other supporting cybersecurity related definitions:</u></p> <p><i>Managed services (or hosted cybersecurity)</i></p> <p>Provision to clients of services such as ongoing third party management/assurance of the cybersecurity/resiliency of clients' systems, networks and information—including continuous monitoring, threat/attack detection and incident response—for clients which choose to out-source such functions to a third party.</p> <p>Such services may also include responsibility for the installation of associated hardware/appliances and software; as well as the configuration, integration, operation and maintenance of comprehensive up-to-date cybersecurity solutions for clients that choose to out-source IT infrastructure and cybersecurity functions to a third party.</p> <p>Examples of related outsourced security support services may include, but not be limited to:</p> <p>Security Information and Event Management (SIEM), Data Loss Prevention (DLP), intrusion detection systems (IDS) / intrusion prevention systems (IPS), threat analytics, vulnerability management, hunt, incident response, and Chief Information Security Officer (CISO) services.</p>	

Canada 