Innovation, Science and Economic Development Canada
Innovation, Sciences et Développement économique Canada
Canada

STATISTICAL OVERVIEW OF CANADA'S CYBERSECURITY INDUSTRY IN 2018

October 2020

Context: Development of relevant, quality and timely cybersecurity industry strategic information to inform policy and industry decision makers

- **Canada** is the first among OECD countries to conduct an **in-depth Government Statistical Agency survey** on cybersecurity industry capabilities from the supplier perspective
  - Complimentary to the Statistics Canada '*Survey of Cybersecurity and Cybercrime*' (user perspective)
- Supported by a multi-year collaborative analytics agreement with industry associations

CADSI · ACTIS | CATAAlliance | Council of Canadian Innovators / Conseil canadien des innovateurs | TECHNATION CA

- This report presents a **statistical overview** of **Canada's cybersecurity industry activities in 2018**, based on the most recent data available
- As such, these findings provide insights into the state of Canada's cybersecurity industry **prior to the onset of the COVID-19 pandemic**
- The next iteration of the biennial survey will measure 2020 industrial activities, and will reflect potential impacts of the pandemic on the cyber security industry in 2020
  - Publication of the basic 2020 data by Statistics Canada is currently scheduled for early 2022

Project Framework

I. Concept Definition (December 2017 – February 2019):

- Consultation with industry, subject matter experts, defence and public security organizations, and policy makers to develop the research framework and the targeted population*

II. Data Development (March 2019 – December 2019):

- ISED sponsored Statistics Canada biennial survey with **completion a legal requirement** under the Statistics Act
- **Data quality validation and firm level imputation** based on administrative data

III. Data Analytics (January 2020 – September 2020):

- Data framework and analytics development
- Economic impact methodology informed by **experts** at the OECD and Statistics Canada
- Development of an overview of the Canadian cybersecurity industry (2018)

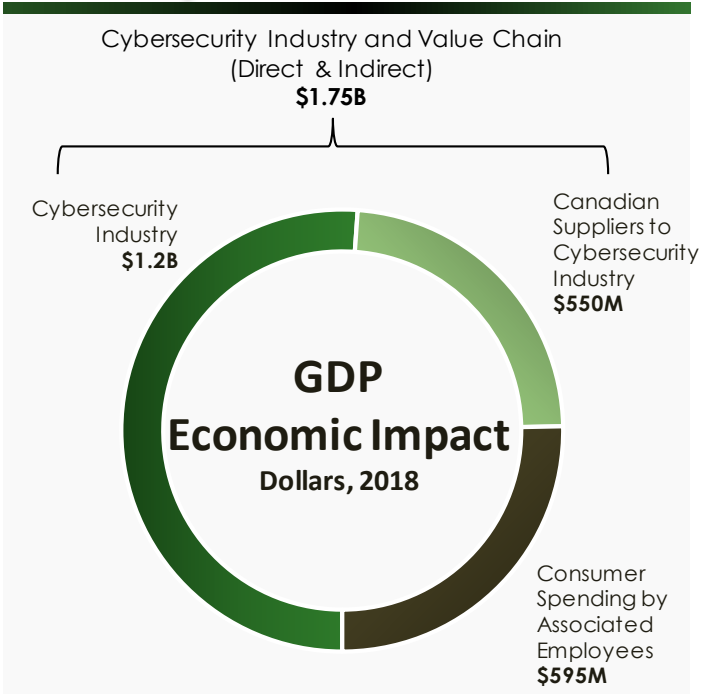
* Targeted population includes firms of all sizes identified by all project partners. In addition, a Census approach of all firms with more than 20 employees across all related Information and Communication Technology (ICT) industries was used to supplement the survey list

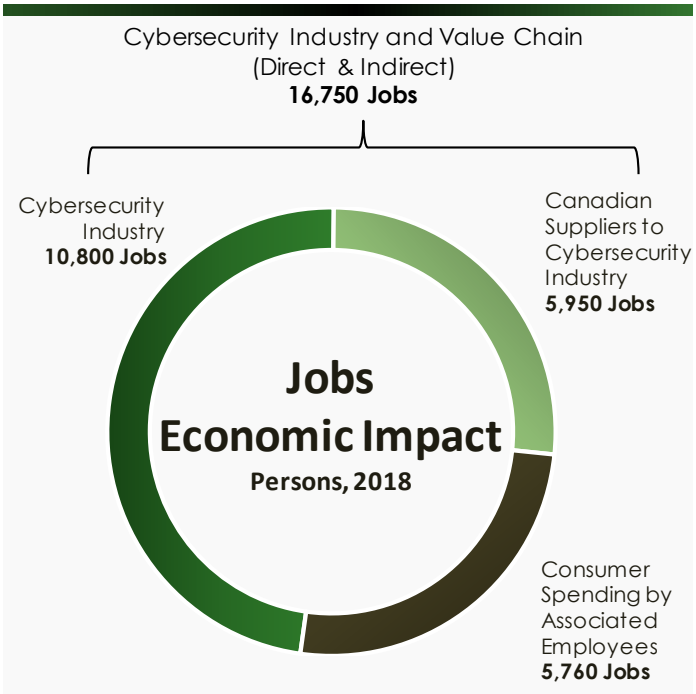
Overview

Core areas of research and analysis

- Economic Impact
- Skills and Diversity
- Size of Firm Footprint
- Regional Areas of Strength
- Exports
- Innovation
- Annex

The Canadian cybersecurity industry contributed over **$2.3B in GDP** and **22,500 jobs** to the Canadian economy in 2018

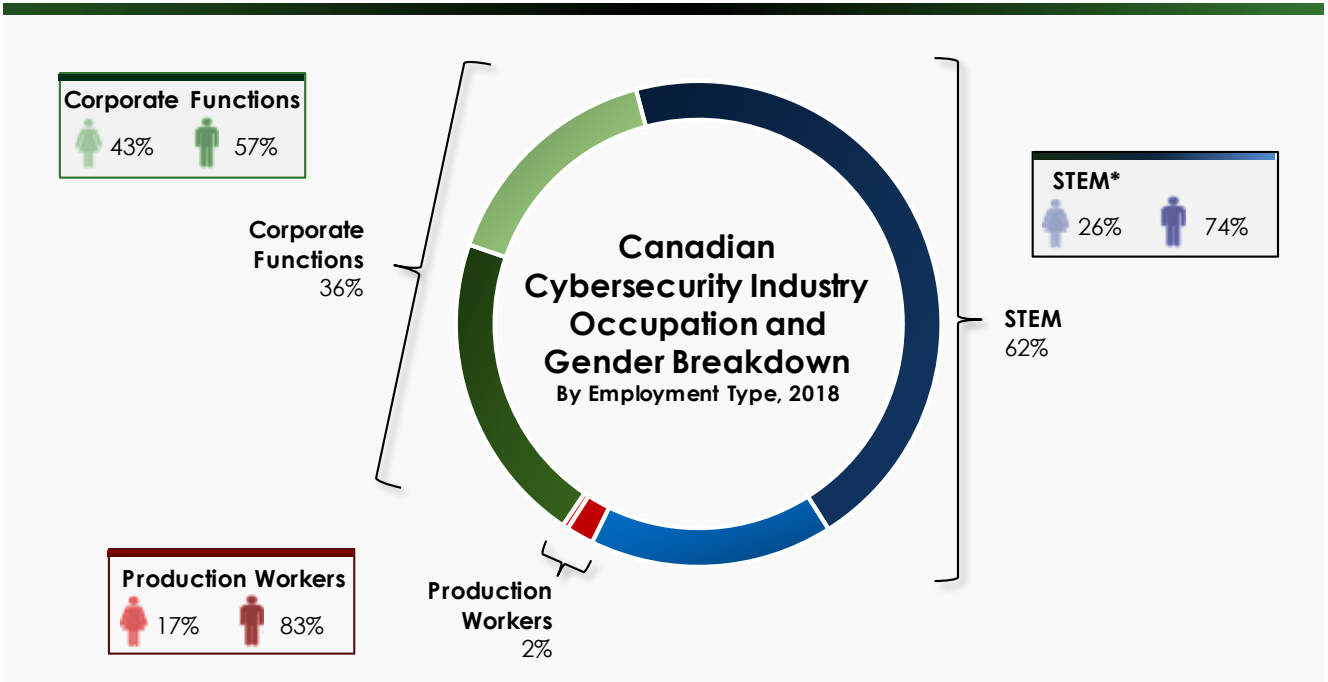




- The cybersecurity industry and its value chain contributed **over $1.7 billion in GDP** and **16,750 jobs** to the Canadian economy (direct and indirect)
- Consumer spending by associated employees contributed an additional **$595 million to GDP** and supported **5,760 jobs** (induced)

Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020; ISED economic modelling based on Statistics Canada's latest Input-Output multipliers (2016) and closest related specific economic impact multipliers that relate to the cybersecurity industry

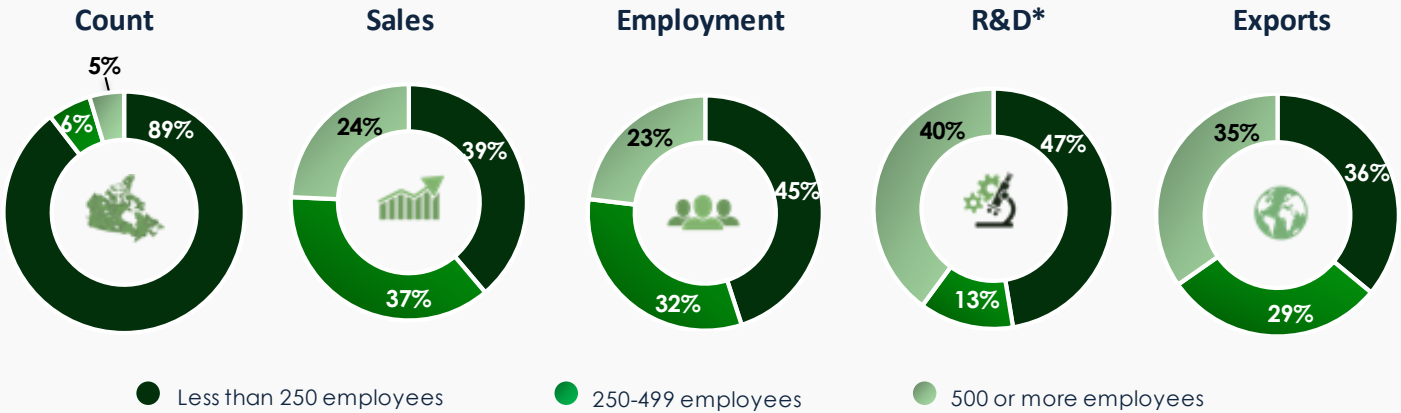
STEM* captured **over 60%** of the industry's total employment in 2018



- The share of **STEM-related occupations** was **more than 65% higher** than **the Canadian ICT industry average****

Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020; Statistics Canada Labour Force Survey (2018), 2020; Innovation, Science, Economic Development Canada, "Canadian ICT Sector Profile 2018", 2020
* STEM : Science, Technology, Engineering, and Mathematics
** See Annex 2 for ICT Industry definitions

Close to 90% of Canadian cybersecurity industry **firms** had **less than 250 employees in 2018**



- In contrast to most industries, **firms with less than 250 employees** captured **more than 45% of industry employment** and **R&D activity** while being responsible for **more than 35% of the industry's exports**

Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020
* R&D spending relates to R&D performed internally by cybersecurity businesses

Breakdown of Canadian cybersecurity industry activities in 2018

Total sales reached close to **$2.9B** across **344 firms**

Types of Products or Services	Share of Total Cybersecurity Sales (%)
Infrastructure Solutions: Cybersecurity infrastructure services and solutions for the ongoing protection of networks and data	50.7%
Bundled Solutions: Cybersecurity solutions based on a single package of services, software and/or hardware involving elements of several other specified cybersecurity categories	11.9%
Encryption	9.0%
Compliance Audits and Program Development: Compliance audits & program development, strategy development, and related risk management and consulting services	8.0%
Industrial Control systems (ICS): supervisory control and data acquisition (SCADA) and operation technology (OT) related cybersecurity	5.4%
Penetration Testing and Threat Monitoring: Penetration testing and associated vulnerability & threat assessments, cyberspace threat monitoring, detection, intelligence services, and active cyber defence measures	4.2%
Forensics and Investigation: Forensics and the investigation of, and response to, cyber-attacks or other cyber incidents and intrusions	1.7%
Training: Cybersecurity Training	0.3%
Other: cybersecurity related goods & services	8.8%
Total Cybersecurity Industry	**100.0%**

Source: Canadian Defence, Aerospace, Marine, and Cybersecurity Industries Survey (2018), 2018 survey released in 2020

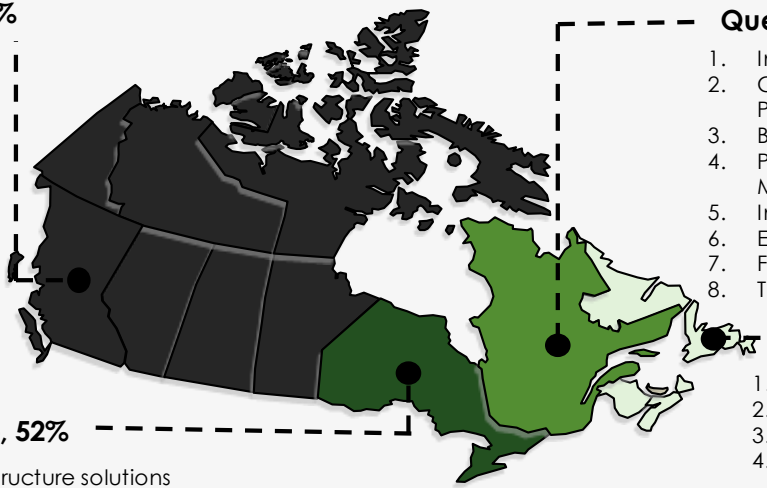
The cybersecurity industry was present across Canada with regional specializations* in 2018

Canadian Cybersecurity Industry Regional Breakdown

By Employment Share, 2018

Western Canada, 24%

1. Infrastructure solutions
2. Compliance Audits and Program Development
3. ICS
4. Bundled Solutions
5. Penetration Testing and Threat Monitoring
6. Encryption
7. Forensics and Investigation
8. Training



Quebec, 19%

1. Infrastructure solutions
2. Compliance Audits and Program Development
3. Bundled Solutions
4. Penetration Testing and Threat Monitoring
5. Industrial control systems (ICS)
6. Encryption
7. Forensics and Investigation
8. Training

Atlantic Canada, 5%

1. ICS
2. Infrastructure solutions
3. Bundled Solutions
4. Compliance Audits and Program Development
5. Penetration Testing and Threat Monitoring
6. Encryption
7. Forensics and Investigation
8. Training

Ontario, 52%

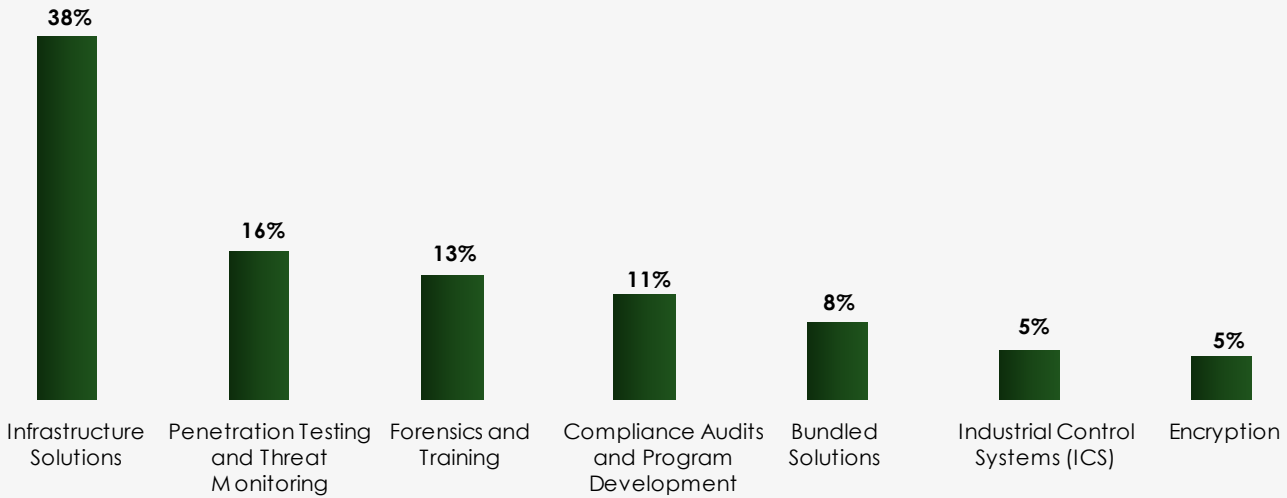
1. Infrastructure solutions
2. Bundled Solutions
3. Encryption
4. Compliance Audits and Program Development
5. Penetration Testing and Threat Monitoring
6. Industrial control systems (ICS)
7. Forensics and Investigation
8. Training

* See Annex 5 for the full titles of the cybersecurity goods and services categories

Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020

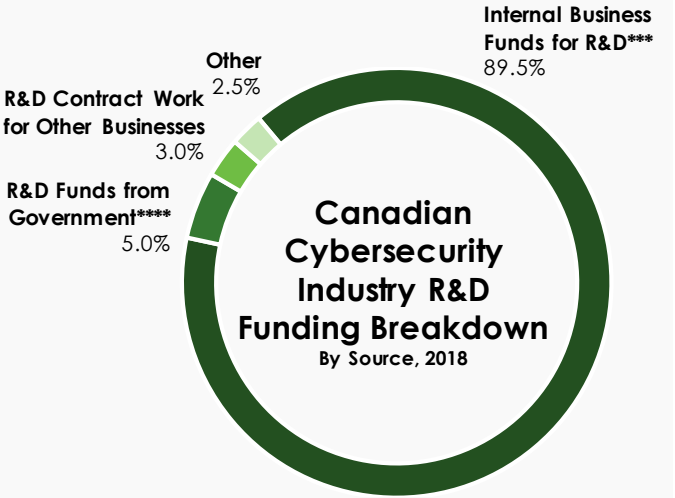
Close to 30%* of total cybersecurity sales were directed to militaries, law enforcement, intelligence and national security agencies in 2018

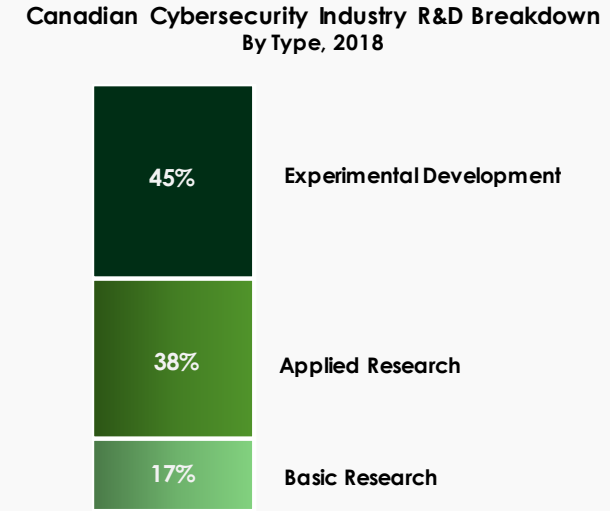
Intensity of sales to military and security agencies by types of products and services, 2018**



Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020
* Includes other cybersecurity related goods & services
** The "Other cybersecurity" activities category is excluded from this chart

The cybersecurity industry's **R&D intensity*** was more than **3X** that of the total Canadian ICT industry average** in 2018





- With **close to $260M** in R&D investment, **over 90% of the R&D performed by the cybersecurity industry** was funded by **industry**
- The **composition** of the cybersecurity industry's overall **R&D activity by type** was **different** from that of Canada's ICT industry**

Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020; and Statistics Canada online Table: 27-10-0344-01 (formerly CANSIM 358-0521)

* R&D intensity is calculated using the ratio of R&D to GDP

** See Annex 2 for ICT Industry definitions

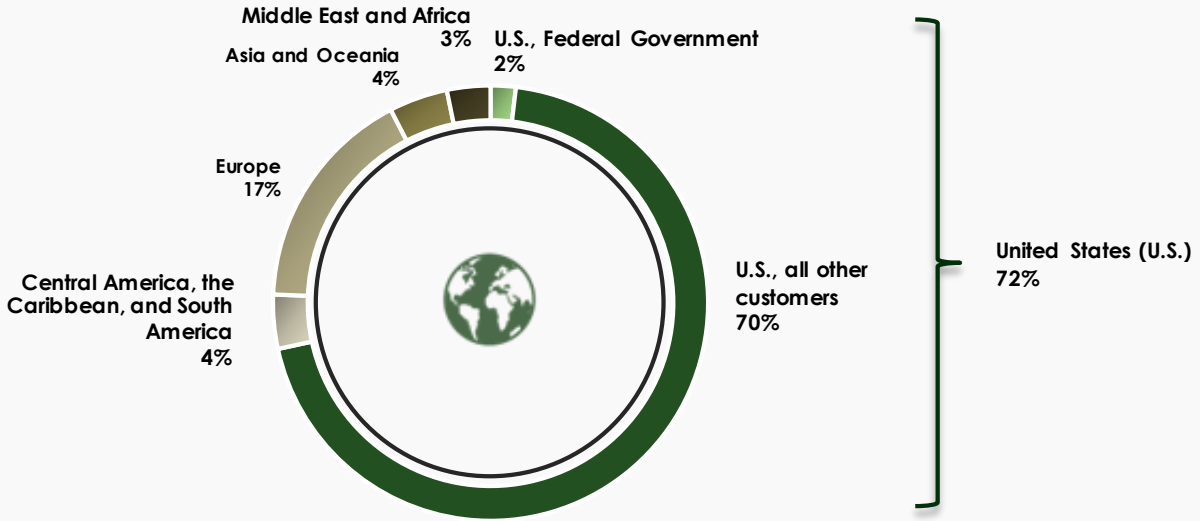
*** This includes funds from the cybersecurity businesses performing the R&D, plus some funds from their parent, affiliated and subsidiary companies

**** Government funded R&D is dominated by grants

Close to $1.1B of cybersecurity **exports** in 2018

Canadian Cybersecurity Industry Global Market Breakdown

By Sales, 2018

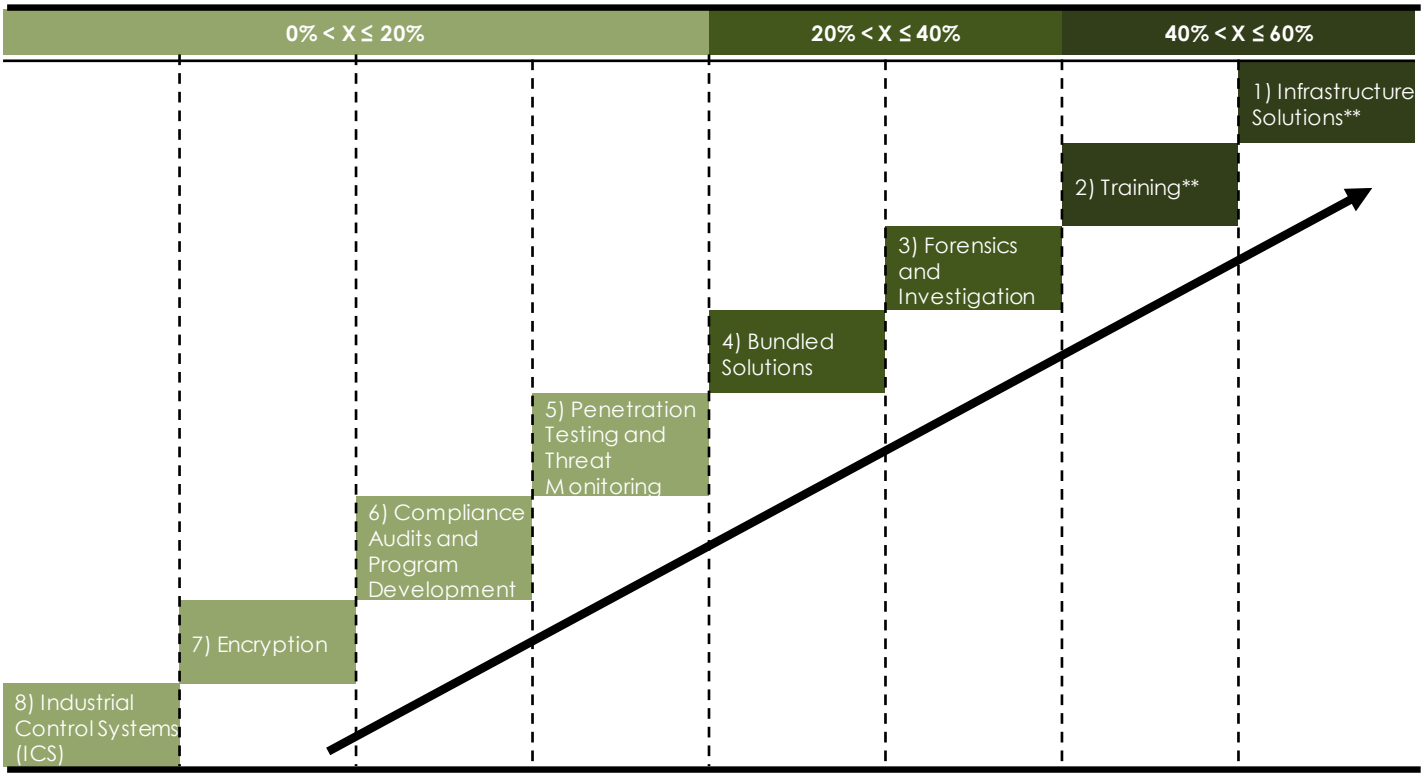


- **Export intensity** was **3X higher** compared to the Canadian ICT Industry average*

Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020
* See Annex 2 for ICT Industry definitions

Export intensity varied greatly by type of products and services in 2018

Export Intensity Ranking of Cybersecurity Activities*, 2018



Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020
* The 'Other cybersecurity' activities category is excluded from this table
** Training and Infrastructure Solutions activities were tied with regards to their export intensities

Key findings

In 2018, the Canadian cybersecurity industry was:

- Generating close to **$2.9B** in cyber sales by **344 firms** across various activities
- Contributing close **22,500 jobs** to the Canadian economy
- Innovative, investing **close to $260 million** in **R&D**
- Highly skilled with **more than 60%** of its workforce relating to STEM
- Globally engaged with **$1.1 billion in exports**
- Supported by **firms with less than 250 employees** for its innovation and export capacities

Annex

Annex 1: Economic Impact Methodology Principles

Annex 2: Canadian ICT Industry Definition

Annex 3: Regional Ranking of Activities

Annex 4: Data Tables

Annex 5: Cybersecurity Industry Definition

Annex 1: Economic Impact Methodology Principles

- Foundation data is based on the latest (2018) Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey released in 2020
- ISED economic modelling based on Statistics Canada's latest Input-Output multipliers (2016) and closest related specific economic impact multipliers that relate to cybersecurity activities
- Economic model is based on Statistics Canada Input-Output (I/O) multipliers
    - Cybersecurity activity has been linked to the latest (2016) and most relevant specific economic impact multipliers per cybersecurity products and services category
    - GDP impact is reported cumulatively and on a yearly average basis
    - Job impact is reported on the 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, 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
    - Totals may not add up to 100% due to rounding

Annex 2: Canadian ICT Industry

ICT manufacturing
- Computer and peripheral equipment
- Communications equipment
- Electronic components
- Audio and video equipment
- Magnetic and optical media

ICT wholesaling

Software and computer services
- Software publishers
- Computer systems design
- Data processing
- Electronic and precision equipment repair and maintenance

Communications services
- Wireless telecommunications carriers
- Wired telecommunications carriers
- Cable and other program distribution

Source: Innovation, Science, Economic Development Canada, "Canadian ICT Sector Profile 2018" (2019), 2020

Annex 3: Regional Ranking of Activities

Ranking	Western and Northern Canada Ranking of Activities
1	Infrastructure solutions
2	Compliance Audits and Program Development
3	Industrial control systems (ICS)
4	Bundled Solutions
5	Penetration Testing and Threat Monitoring
6	Encryption
7	Forensics and Investigation
8	Training

Ranking	Ontario Ranking of Activities
1	Infrastructure solutions
2	Bundled Solutions
3	Encryption
4	Compliance Audits and Program Development
5	Penetration Testing and Threat Monitoring
6	Industrial control systems (ICS)
7	Forensics and Investigation
8	Training

Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020

Annex 3: Regional Ranking of Activities (cont.)

Ranking	Quebec Ranking of Activities
1	Infrastructure solutions
2	Compliance Audits and Program Development
3	Bundled Solutions
4	Penetration Testing and Threat Monitoring
5	Industrial control systems (ICS)
6	Encryption
7	Forensics and Investigation
8	Training

Ranking	Atlantic Canada Ranking of Activities
1	Industrial control systems (ICS)
2	Infrastructure solutions
3	Bundled Solutions
4	Compliance Audits and Program Development
5	Penetration Testing and Threat Monitoring
6	Encryption
7	Forensics and Investigation
8	Training

Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020

Annex 4: Data Tables

Table I: Economic Impact

GDP Economic Impact ($M)				
Cybersecurity Industry ($M)	Suppliers to Cybersecurity Industry ($M)	Cybersecurity Industry and Value Chain ($M)	Consumer Spending by Associated Employees ($M)	Cumulative Total GDP ($M)
$1,200M	$550M	**$1,750M**	$595M	**$2,345M**

Job Economic Impact				
Cybersecurity Industry	Suppliers to Cybersecurity Industry	Cybersecurity Industry and Value Chain	Consumer Spending by Associated Employees	Total Annual Average Jobs
10,800 Jobs	5,950 Jobs	**16,750 Jobs**	5,760 Jobs	**22,500 Jobs**

Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020; ISED economic modelling based on Statistics Canada's latest Input-Output multipliers (2016) and closest related specific economic impact multipliers that relate to cybersecurity activity

Annex 4: Data Tables (cont.)

Table II: Regional Breakdown

Regional Breakdown	Western and Northern Canada	Ontario	Quebec	Atlantic Canada
Distribution of Employment in the Cybersecurity Industry	24%	52%	19%	5%

Table III: Intensity of sales to military and security agencies by types of products and services, 2018

Categories	Intensity of sales to military and security agencies by types of products and services, 2018
Infrastructure solutions	38%
Penetration Testing and Threat Monitoring	16%
Forensics and Training	13%
Compliance Audits and Program Development	11%
Bundled Solutions	8%
Industrial Control Systems (ICS)	5%
Encryption	5%

Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020

Annex 4: Data Tables (cont.)

Table IV: Firm Size Breakdown

Size Breakdown	Share of Total Cybersecurity Industry Enterprise Counts	Share of Total Cybersecurity Industry Sales	Share of Total Cybersecurity Industry Employment	Share of Total Cybersecurity Industry R&D	Share of Total Cybersecurity Industry Exports
Enterprises with less than 250 employees	89%	39%	45%	47%	36%
Enterprises with between 250 and 499 employees	6%	37%	32%	13%	29%
Enterprises with 500 or more employees	5%	24%	23%	40%	35%
Total Enterprises	**100%**	**100%**	**100%**	**100%**	**100%**

Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020

Annex 4: Data Tables (cont.)

Table V: Occupation and Gender Breakdown

Occupation Breakdown	Share of Employment by Occupation	Occupation & Gender Breakdown	Share of Occupations' Employment by Gender
STEM	61%	STEM Male	74%
		STEM Female	26%
Production Workers	2%	Production Worker Male	83%
		Production Worker Female	17%
Corporate Functions	36%	Corporate Functions Male	57%
		Corporate Functions Female	43%

Table VI: Sources of Funds for R&D

Sources of R&D	Share of R&D Breakdown
Internal Business Funds for R&D	89.5%
R&D Funds from Government	5.0%
R&D Contract Work for Other Businesses	3.0%
Other	2.5%

Types of R&D	Share of R&D Breakdown
Basic Research	17%
Applied Research	38%
Experimental Development	45%

Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020

Annex 4: Data Tables (cont.)

Table VII: Domestic and Foreign Market Breakdown

Cybersecurity Domestic Sales	63%	Cybersecurity Export Sales	37%
Domestic Sales by Customer Type*		***Export Sales by Destination***	
• Canadian Federal Government	13%	• United States	72%
• Other Canadian Customers	87%	• Europe	17%
		• Asia and Oceania	4%
		• Central America, the Caribbean, and South America	4%
		• Middle East and Africa	3%
Cybersecurity Domestic Sales Total	**100%**	**Cybersecurity Export Sales Total**	**100%**

Source: Canadian Defence, Aerospace, Marine, and Cybersecurity Industries Survey (2018), 2020
* Breakdown of total domestic sales between domestic customers excludes customer breakdown that is unspecified

Annex 5: Cybersecurity Industry Definition

Definition of Cybersecurity Categories

Cybersecurity

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.

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.

Solutions may **include** or relate to, but not necessarily be limited to:

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.

Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020

Annex 5: Cybersecurity Industry Definition (cont.)

Definition of Cybersecurity Categories

Cybersecurity Solutions Based on a Single Package of Services, Software and/or Hardware—and Involving Elements of Several of the Other Cybersecurity Categories as Specified Under this Survey

This category **includes** sales spanning both goods and/or services (including research, development, design, engineering, testing & evaluation services) relating to:

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 survey's other specified cybersecurity goods and services categories and associated functions, tasks.

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.

Encryption

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:

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).

Excluding:

integration or resale of commercial encryption is not to be **included** here;

encryption that is primarily **included** under another goods & services category.

Compliance audits & program development, strategy development, and related risk management and consulting services

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:

cybersecurity audits / compliance audits;

cybersecurity strategy development;

cybersecurity compliance program development;

other related risk management and consulting services.

Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), and Operation Technology (OT) Related Cyber Security

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:

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.

Excluding protection of enterprise IT networks.

Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020

Annex 5: Cybersecurity Industry Definition (cont.)

Definition of Cybersecurity Categories

Penetration testing and associated vulnerability & threat assessments, cyberspace threat monitoring, detection, intelligence services, and active cyber defence measures

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:
Penetration testing;
Vulnerability assessments.

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.

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.

Forensics and the investigation of, and response to, cyber attacks or other cyber incidents and intrusions

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 software tools involved in identifying, assessing, and responding to cyber-attacks and incidents. Examples may **include**, but not necessarily be limited to:
network forensics;
related hunt services & tools;
fraud analytics;
identification of inside perpetrators;
other incident response services.

Cybersecurity training

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:
training;
workforce development;
educational services or solutions.
This **includes** all levels, from more basic users to advanced practitioners; and spans services, courseware, software, or other delivery mechanisms.

Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020

Annex 5: Cybersecurity Industry Definition (cont.)

Definition of Cybersecurity Categories

Other cybersecurity related goods & services

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:

Other activities that could be considered cybersecurity related in nature, (including those beyond just defensive or passive cybersecurity related activities).

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.

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.

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 whole sale activities.

Other cybersecurity related definitions:

Managed services (or hosted cybersecurity)

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.

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.

Examples of related outsourced security support services may **include**, but not be limited to:

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.

Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2018), 2018 survey released in 2020


Canada