HILL DAY 2022

Equipping and Building the Capacity for Our Digital Nation

Presented By:

TECHNATION[CA]

RECENT STATS

By 2025,
ICTC forecasts employment in the Canadian digital economy to reach
2.26 million -
triggering a demand for an additional 250,000 jobs.

Globally, the number of ransomware attacks shot up by
151%
in the first half of 2021.

Worldwide spending on information security and risk management technology and services is forecast to grow
12.4% to reach $150.4 billion (USD) in 2021[1].

Canada is facing a
talent deficit
that is limiting our ability to harness the full potential of emerging technology. Demand for cyber talent is estimated to be increasing by
7% every year[2].

Supply chain attacks rose by
42% in the first quarter of 2021
in the US- disproportionately impacting businesses that work with governments, and impacting up to seven million people[3].

According to CSE and the Cyber Centre,
the number of cyber threat
actors is rising, they are becoming more sophisticated and state-sponsored cyber threats are increasing[4].

Since March 2020, nearly
25% of all Canadian
small businesses have experienced some kind of hostile cyber incident. The rate of cyber incidents per 100,000 citizens also went up from 73 to 168 between 2016 and 2020. $106 million were lost in Canada due to scams and frauds in 2020[5].

1. Source: "Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 billion in 2021"- Gartner
2. Source: Cybersecurity Report "The Changing Faces of Cybersecurity- Closing the Cyber Risk Gap" – Deloitte
3. Source: MORE Alarming Cybersecurity Stats For 2021 ! (forbes.com)
4. Source: ncta-2020-e-web.pdf (cyber.gc.ca)
5. Source: 14 Scary Canadian & Global Cyber Crime Statistics for 2021"- Reviewlution.ca

OUR DIGITAL NATION IS AT RISK:

Digital technologies have become essential to our way of life, but with their adoption we open ourselves up to threats.

The Communications Security Establishment (CSE) and its Canadian Centre for Cyber Security (CCCS) has warned about state-sponsored actors targeting Canada's critical infrastructure, such as our electricity grid. The cost of a successful attack on major supply chains or Canada's critical infrastructure could be enormous.

Cybercrime is already estimated to cost Canada over $3 billion a year. Internationally, the annual cost is estimated at $6 trillion (USD), and expected to rise to $10 trillion (USD) by 2025.

The cost of cybercrimes is a drain on organizations' finite resources and decrease their competitiveness against their peers.

Budget 2021 announced $1.5 billion in new investments into federal government cyber security enhancements including an $80 million investment in the Cyber Security Innovation Network.

In fact, surveys have shown that 92% of Canadians believe the federal government needs to prioritize investments in cybersecurity[1].

But more funding alone isn't the answer to this national challenge. We need to address the talent gap as well.

TECHNATION's Cyber Security Skills Framework identifies four key workforce development challenges for Canadian businesses right now:

- Generating and retaining cybersecurity operations talent to meet the needs of the Canadian labour market.
- Ensuring contributing technical and non-technical roles have required knowledge, skills, and abilities.
- Being responsive to the changing technology landscape
- Normalizing cybersecurity work and activities within the Canadian workplace.

Canada's tech sector can help....

A 'Team Canada' approach that leverages the best minds and technological capabilities available is what's needed.

Canada's cyber industry contributes $2.3 billion to GDP and employs over 22,000 Canadians[2]. More than 340 firms build best-in-class technology sourced around the world including all 5 eyes allies[3].

1. Source: Angus Reid Institute Survey: Advancing online government service: Canadians open to more & better access; concerned about cybersecurity- Angus Reid Institute
2. Source: Statistics Canada
3. Source: Statistical Overview of Canada's Cyber Security Industry in 2018, ISED, 2020.

OUR CHALLENGE TO THE GOVERNMENT: TO EQUIP AND BUILD THE CAPACITY FOR OUR DIGITAL NATION.

When it comes to Canada's national cybersecurity posture, our cyber security industry wants to work collaboratively and help. **TECHNATION is challenging the federal government to:**

Significantly enhance federal investments in its own cyber security, and cyber security for businesses:

- Canada's current level of investment is not sufficient to secure our economy, critical infrastructure, and government enterprises.

The Government of Canada should secure its own enterprise and lead by example:

- The Government of Canada continues to buy roughly 90% of its cyber technology from large multinational suppliers. The best response to cyber threats is one that mobilizes the innovation potential of not only multi-national firms, but also our strong domestic industry, especially Small and Medium Enterprises (SMEs).
- Cybercrime (ransomware) and nation state are the two most prevalent threats to our country right now. The need for cyber security measures – for government, businesses and individuals alike – is an absolute necessity. The Government of Canada needs to improve collaboration with industry, infrastructure and reporting mechanisms.

As you develop and renew the National Cyber Security Strategy and associated cyber action plan, we would urge the government to:

- Engage Canada's leading cyber security industries and experts to participate in a bi-annual meeting between industry and the Ministerial Committee to discuss tangible results.

The Government of Canada should urgently address cyber talent shortages by:

- Stimulating the development of strategies, approaches, and techniques to more rapidly increase the supply of qualified cybersecurity workers.
- Nurturing a diverse learning community through creative efforts that increase the number of un-derrepresented populations in the cybersecurity workforce.
- Inspiring cybersecurity career awareness, stimulate exploration, and enable preparedness with students in K-12.
- Providing support to organizations to address market demands by providing tools and techniques that enhance recruitment, hiring practices, development, and retention of cybersecurity talent.