Cyber.
Right. Now.

Leading the global cybersecurity future

Open Letter: Ottawa needs to get serious about cybersecurity. Right. Now.

Canada's political leadership must get more engaged and serious about Canadian cybersecurity, now.

Canadians are more worried about falling victim to a cyber-attack than just about anything else, including COVID and climate change, according to the 2021 Edelman Trust Barometer. And who can blame them? Cyber criminals have successfully, and repeatedly, targeted our critical infrastructure including our hospitals, schools, transit systems, and local and federal governments causing significant disruption to essential services.

Not only were essential services exponentially disrupted, but these attacks resulted in the harmful exposure and at times irreversible loss of sensitive data that includes health information, vital intellectual property, and highly personal information about our finances — and even our children. The federal government's chief of Communications Security Establishment (CSE), Shelly Bruce has gone on record stating that cybercrime is the "most prevalent, most pervasive threat to Canadians and Canadian businesses." What more needs to happen to prompt government to get serious about cybersecurity?

These sorts of attacks have been escalating over the past few years, and the vast majority of Canadians are calling for urgent action to secure Canada's public and private IT systems. According to a recent Angus Reid Institute survey, 92 percent of Canadians say the federal government needs to prioritize investments in cybersecurity.

As members of the Canadian Chamber of Commerce *Cyber. Right. Now*. campaign, we urge the Government of Canada to raise the bar on cybersecurity in the 2022 federal budget by undertaking the following three actions to ensure that our infrastructure is resilient to cyber-attacks and that our economy can continue to grow as one of the world's most innovative, vibrant and secure places to do business.

- **Secure critical infrastructure, supply chains, and businesses of all sizes** from cyber threats by investing in cybersecurity on par with our G7 peers;
- **Grow the economy** by accelerating the commercialization of cybersecurity innovation in Canada and with our trading partners; and
- **Bolster Canada's cybersecurity workforce** by investing in cybersecurity education, talent development, retention and programs that diversify and expand the cyber workforce.

The goal of the *Cyber. Right. Now.* campaign, backed by over two dozen of Canada's leading technology companies and cybersecurity organizations from across the country, is to make Canada a world leader in cybersecurity. We believe that every individual and organization in Canada deserves robust protection against cyber threats, which are only increasing in complexity and scale. Canadian companies, businesses of all sizes and technology leaders from all walks of life are eager to contribute their expertise to combat this persistent and growing threat.

To give credit where it's due, the federal government to-date has provided about $1.5 billion total in funding to the Canada Revenue Agency, Economic and Social Development Canada, the Communications Security Establishment, and Shared Services Canada in Budget 2021 to bolster some parts of the government's own cyber defences. This was important. But the scope for the funding was very narrow and the dollar figure will not sufficiently address the scope of Canada's weaknesses. Even if the federal government were to only concern itself with its own safety (which would be unwise), the approach is still far too narrow. Consider that organizations conducting business with the federal government are prime targets of supply chain attacks and saw a significant increase of 42% in the first quarter of 2021. For example, weak links in the supply chain in the United States allowed hackers to exploit and gain control of the Solar Winds infrastructure and Colonial Pipelines, which significantly impacted critical infrastructure for months.

Protecting Canadians means more than just protecting the federal government.

With the pace of digitalization accelerating globally – especially since March 2020 – Canada simply cannot afford to leave our businesses, infrastructure and communities exposed to cyber threats. Cybersecurity has never been more vital to both our country's national security and economic potential.

A spotlight on cybersecurity in the 2022 federal budget can help position Canada as a global leader in cybersecurity. It's time for Ottawa to demonstrate that the government understands the full scope of the challenge before us and is seriously committed to addressing it nationally.

The time to act on cybersecurity is right now.

--

This open letter is from the Canadian Chamber of Commerce Cyber. Right. Now. campaign. The campaign is supported by, BlackBerry, Microsoft Canada, Cisco, Amazon Web Services (AWS), Calian, eSentire, General Dynamics Mission Systems-Canada, Innovapost, Terranova Security, Beauceron Security, the Canadian Cyber Threat Exchange, Communitech, CyberNB, the Rogers Cybersecure Catalyst, Cycura, CYDEF, Difenda, F12.net, Field Effect, FWDSEC, Hitachi ID, Idealogical Systems Inc., Nirico Systems Inc., the Institute for Cybersecurity & Resilient Systems at Ontario Tech, OPTIV, RHEA Group, RiskAware, rSolutions, Turbo IT, and the Women CyberSecurity Society.