EXECUTIVE SUMMARY

The federal government is failing to protect Canadians from increasingly sophisticated cyber attacks that have already victimized millions.

In 2017 alone, over 10 million Canadians had their personal information compromised through targeted attacks and — more often — through cyber operations directed against businesses that hold Canadians' private information.

Banking information, internet activity, social insurance numbers, family photos — this wealth of intimate data is up for grabs by malevolent actors who can steal your life from the other side of the world.

That's just the personal side.

Hackers have held hospitals hostage by encrypting their critical systems and demanding money to restore them; a quick glance at news headlines south of the border suggests that sinister groups are trying to use technology to sway elections.

To date, Canada has offered only limp responses to this real and rising threat.

The Office of the Privacy Commissioner of Canada, for instance, is responsible for protecting and promoting privacy rights — but it doesn't even have the power to make companies comply with legislation designed to protect Canadian consumers, or to impose fines when companies breach that legislation.

Police, too, are relatively powerless against the relentless and creative onslaught of cyber scams. Royal Canadian Mounted Police officers told the committee that cyber crime continues to be underreported; the many different approaches criminals use also make it difficult for police to develop a coordinated response.

The federal government should be leading efforts to make Canadians' information more secure but there is as yet no single, national standard for cyber security, even when it comes to critical infrastructure.

Meanwhile, cyber criminals have an ever-expanding network of paths into Canadians' homes. The "Internet of Things" offers an enticing assortment of web-connected items like video baby monitors, fridges and automated vehicles. Few if any of these items, however, are designed to prioritize security.

That means a criminal could sell video footage of your child in his bedroom to the highest bidder, or take control of your vehicle from half a world away. The convenience and increasing ubiquity of this technology comes with grave risks to unwitting users.

Ultimately, education is the best way to keep safe. Being aware of the nature of common threats allows people and businesses to take steps to secure themselves. But the success of cyber-criminal enterprises shows the extent to which Canadians have yet to embrace the adage: to be forewarned is to be forearmed.

KEY RECOMMENDATIONS

It is imperative that the federal government act swiftly and decisively to deprive cyber criminals of the advantages they continue to enjoy. This report makes a number of specific recommendations, based on the testimony of expert witnesses, to help the government defend its citizens.

First, the committee believes that **all levels of government must prioritize cyber security education as part of the national cyber security strategy**. To that end, senators recommend that the federal government create a national cyber literacy program, led by the Canadian Centre for Cyber Security, to educate consumers and businesses about how to protect themselves. The government should also create a new national centre of excellence in cyber security and expand two existing centres to promote university-level research and encourage Canadians to pursue careers in cyber security-related fields.

The committee also urges the federal government to **modernize Canada's privacy legislation**. This should include empowering the Office of the Privacy Commissioner to make orders and impose fines against companies that fail to protect their customers' information.

As a corollary, the committee believes that **businesses should be given incentives to invest in cyber security improvements**, for example, by making these investments tax deductible.

Ultimately, the committee believes the grave threats cyber crime poses makes it necessary to **create a new federal minister of cyber security**. The minister would coordinate cyber security efforts across all levels of government and help Canadians hold the federal government to account for its efforts to keep Canadians safe.

NEXT STEPS

Governments, businesses and individual Canadians each have a role to play in protecting the country from this cyber scourge. The committee's recommendations, grounded in expert testimony, shows a clear way forward.

The committee will continue to advocate for the recommendations contained in its report in order to hold the federal government to account for its disappointingly ineffective efforts to combat these serious crimes.

Cyber criminals are everywhere. The internet gives them access to virtually anyone. Canada cannot continue to be complacent in the face of this insidious, online criminality.

It should keep you up at night.