Key takeaways:

1. The perpetrators of cybersecurity threats are incredibly savvy for all the wrong reasons, as new technologies emerge, so too are sophisticated cyber threats emerging.

2. Since the pandemic, Cybersecurity incidents have increased 600% worldwide, at an economic cost of 6 trillion dollars.

3. Industry support: MasterCard, for example, has started a new cybersecurity research lab as well as establishing and funding incubators and emerging leadership programs in cybersecurity.

4. Cybersecurity is an international threat, important that countries work together against other state-sponsored cyberattacks.

5. Online business increased exponentially out of the pandemic. To keep up, education needs to be accessible for businesses to be as protective as possible & to look at ways they should mitigate risk.

6. Canadian economy on the whole, small businesses make up near 90% of businesses, so cybersecurity for small and medium sized enterprises is imperative.

7. Multifactor authentication is primary tool for small businesses. Need to equip small businesses with adequate resources to use mitigating technology.

8. Never too small a business to be removed from the threat of cybersecurity. Cybersecurity consultations need to meet small businesses "where they are" and educate from there.

9. Cyberinsurance is a growing market, final line of defense. Like seatbelts when they first were mandated, today we understand that everyone needs a seatbelt.

10. CIRA - As a not-for-profit organization, CIRA has a broader mandate to build a trusted internet in Canada. Leveraging its experience in providing 100% up-time for 3 million .CA domains to provide a suite of cybersecurity services to help protect millions of users across Canada.

11. Need to do a better job of educating to lessen the gap between protocols and practicality. Don't make the perfect the enemy of the good.

12. Build risk plan around cybersecurity.

13. Get small businesses the resources they need, speaking to insurers is an important first step.

14. What is first step if business has a breach? Contact local police or RCMP. Then we need to take the shame out of this, enable reporting about cybersecurity events. Then put protections in place for remaining data in your system.

15. Cybersecurity training is widely available. Do regular phishing and password tests and training for employees. Multifactor authentication is important risk mitigation and helps with insurance, too.

16. Advocacy needs to happen for service providers to play a stronger role in protecting small businesses.

17. Attendee, U.S. consul general to Canada, Susan R. Crystal, suggests building up talent pools and awareness through elementary and secondary education institutions to prepare the next generation.

18. Think about getting to a tipping point where businesses might showcase their cybersecurity mandate as a differentiator, to propel growth in their business.

19. Build an ecosystem that takes care of all stakeholders, having this notion built into partnerships is essential, in the spirit of collaboration = good for all assists in combatting cybercrime globally.