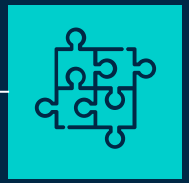
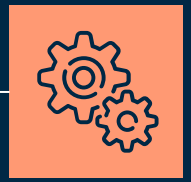
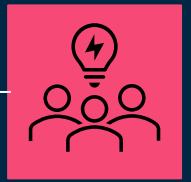
CYBER THREAT INTELLIGENCE IN CANADA

David Macintyre,
Scott Davenport
Jace Stelman

TABLE OF CONTENTS







LITERATURE REVIEW

Consensus Points

Debate

Definition of CTI

"CTI represents actionable threat information that is relevant to a specific organization and that thus demands its close attention. The capability involves foresight and insight, and is intended to identify impending change, which may be positive, representing opportunity, or negative, representing threat" (Shin and Lowery)

METHODOLOGY: CASE STUDY

Analyzing Case Studies through C T I Frameworks

Criteria

Criticality (Impact of Attack)
Targetability (Frequency of Attack)
Vulnerability (Difficulty of Attack)

CASE STUDIES

HEALTH CARE

FINANCE

AGRICULTURE

HIGHER EDUCATION

CASE STUDIES

03

HEALTH CARE

HEALTH CARE SENSITIVE AND TARGETABLE

$1000

Potential Value of a confidential health record on the Darkweb

58%

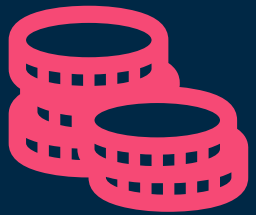
Percent of cyber attacks facilitated by insiders.

29%

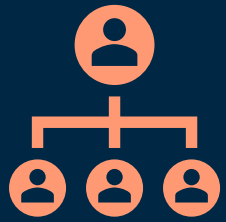
Percent of healthcare workers aware of someone in their organization selling confidential information

HEALTH CARE AND CTI

High risk; highly vulnerable



Threat actors and their motivations:



Organizational and technical challenges

FINANCE

17 mo.
113,154 acc.
3,190 discl.

1,000 comp.
$950,000 US

Bank of Montreal (BMO)

Credit Union

Insurance

FINANCE
DETECTION AND IMPLENTATION BLUNDERS

233 days

To **detect and contain** a breach

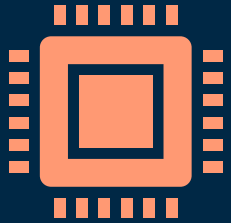
18%

Of all IT implementing and processing errors **among all sectors**

8x

More costly than malicious cyber or privacy and lost data incidents

FINANCE AND CTI



IT implementing and processing errors

Increased digitization

Need to be transparent

AGRICULTURE

EMPIRE
COMPANY LIMITED

$32 M Direct
$15 M Indirect

$23 M Direct

AGRICULTURE MOST UNPROTECTED SECTOR

65%

Of enterprises have cyber protection

12%

Of enterprises are completely unprotected

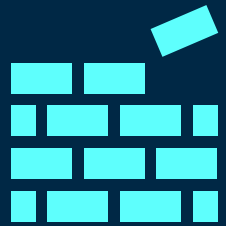
1 in 9

Canadians employed by AG sector

AGRICULTURE AND CTI

Educate on need for cyber security

Increase spending in malware protection



No minimum standards

HIGHER EDUCATION

HIGHER EDUCATION CYBER INCIDENTS ON THE RISE

64%

Large Educational Services Organizations Impacted (2017)

4x an.

Impacted By Theft Of Personal And Financial Information

46%

Of Incidents Disrupted Services Or Functionality

HIGHER EDUCATION
MORE VULNERABILITIES
MORE CHALLENGES

Increased vulnerabilities from Pandemic

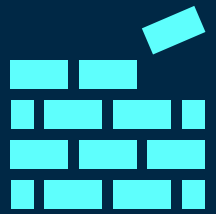
Decentralized IT systems; many points of infiltration

Legal confusion

HIGHER EDUCATION AND CTI

Increase technical capabilities

Increase governmental support



Sector specific guidance on minimum cyber security measures

BROAD GAPS RECOMMENDATIONS

04

TECHNOLOGICAL DEFICIENCIES

Enhance data collection

Training personnel

Equalize technological gaps in underdeveloped sectors

LEGAL GAPS

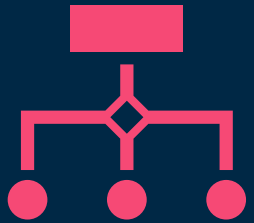
Inadequate legal regimes in Canada

Jurisdictiona
l confusion

Bill C-27

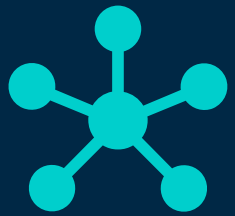
ORGANIZATIONAL GAPS

Military level redundancies VS. Business level efficiency



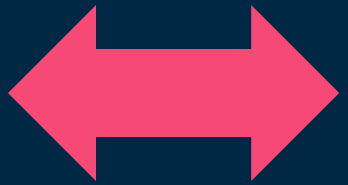
Shift in business organizational structure to improve intelligence

LACK OF TRANSPARENCY



Lack of intelligence sharing

Vertical Information Sharing



Horizontal information sharing

GAPS	RECOMMENDATIONS
Legal Deficiencies	Update Canadian laws to incentivize higher cybersecurity standard
Organizational Deficiencies	Imbed CTI at all levels of business through: • Basic cyber hygiene training for all • IT teams with intelligence training • Cyber landscape understanding for management
Lack of Transparency	Leverage existing cybersecurity organizations Leverage pre-existing business associations to disseminate key intelligence and best practices Use intelligence sharing to build resilience in sectors
IT Challenges	Continued advancement and implementation to cyber security solution

THANK YOU.
QUESTIONS?

David Macintyre,
Scott Davenport
Jace Stelman