CSKA Community Safety Knowledge Alliance
Research to Practice to Alignment

Cyber Security Cooperation Program

Cyber Security Capacity in Canadian Agriculture

Research Summary

April 2022

Funded in part by
Canada

Agriculture is integral to Canada's national economy and to the health and wellbeing of all Canadians.

But, agfood systems and their supply chains, like other critical infrastructures, are under growing threat.

Enhancing the security of digital agricultural production contributes to farm business risk management as well as to farm business management and the overall competitiveness of our agfood sector.

Context

Domestic food security, along with rural economic development and resilience, are key to national prosperity.

Canada is actively positioning itself for global leadership vis à vis innovation, transparency, food security and sustainable development goals.

Consequently, food security can be considered a component of national security.

'Ag 4.0' is changing how we produce and distribute food

Types of digital on-farm technologies

- **Wireless sensor networks**
  - e.g., Soil moisture, animal movement and health
- **Industrial control systems, automated and robotic processes and autonomous and semi-autonomous vehicles and equipment**
  - e.g., GPS controlled seeding and harvesting equipment, environmental & industrial control systems
- **Big data-based decision support systems**
  - e.g., Collection and analysis of farm yield data for decision support
- **Supply chains and farm services**
  - e.g., Supplier deliveries and transactions, food traceability, purchaser systems
- **Energy management systems**
  - e.g., Renewable energy generation supplying power to sensors and charging stations

Farm Network Vulnerabilities

Open Front Door
Common open ports - physical points of connection on computers that allow communication with external devices and to the Internet *(examples: for file transfer, for email retrieval and routing; for access to the World Wide Web; to allow connected applications to communicate with one another)*

Side Window
Using psychological techniques to get people to do things they shouldn't do *(examples: make a payment; click a link; or share confidential information)*

Locked Back Door
Methods for getting around normal physical and computer safeguards *(like user authentication or encryption in a computer or connected device)*

CYBER THREAT ACTOR	MOTIVATION	ATTACK FOCUS
Nation States	Geopolitical, economic and technological power	Disinformation, supply chain control, influence or interference, trade secrets, theft of intellectual property
Cyber Criminals	Profit/privateering for nation state	Financial data, personally identifiable information or ransomware, extortion
Hacktivists	Ideological causes inspired hacking	Sensitive business data, client and supplier data
Extremist Groups	Ideological inspired violence	Disruption of critical systems or data for physical effect
Hackers	Thrill seeking	Penetration and control of systems and devices
Insider Threats	Discontent/retribution	Destruction/damage of business systems or profiteering of intellectual property

Adapted from Canadian Centre for Cyber Security (https://www.cyber.gc.ca/sites/default/files/publications/Intro-ncta-2020_e.pdf)

Cyber Threats to the Agfood System are Real

TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

1 September 2021

Cyber Criminal Actors Targeting the Food and Agriculture Sector with Ransomware Attacks

20 April 2022

Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons

BBC May 20, 2022: *Global food supply chain at risk from malicious hackers*
https://www.bbc.com/news/science-environment-61336659

Cyber attacks have already begun to target key pinch-points in agfood systems

Examples of AgFood attacks in 2021

AWEX we know wool

JBS FOODS

NEW COOPERATIVE INC.

Crystal Valley

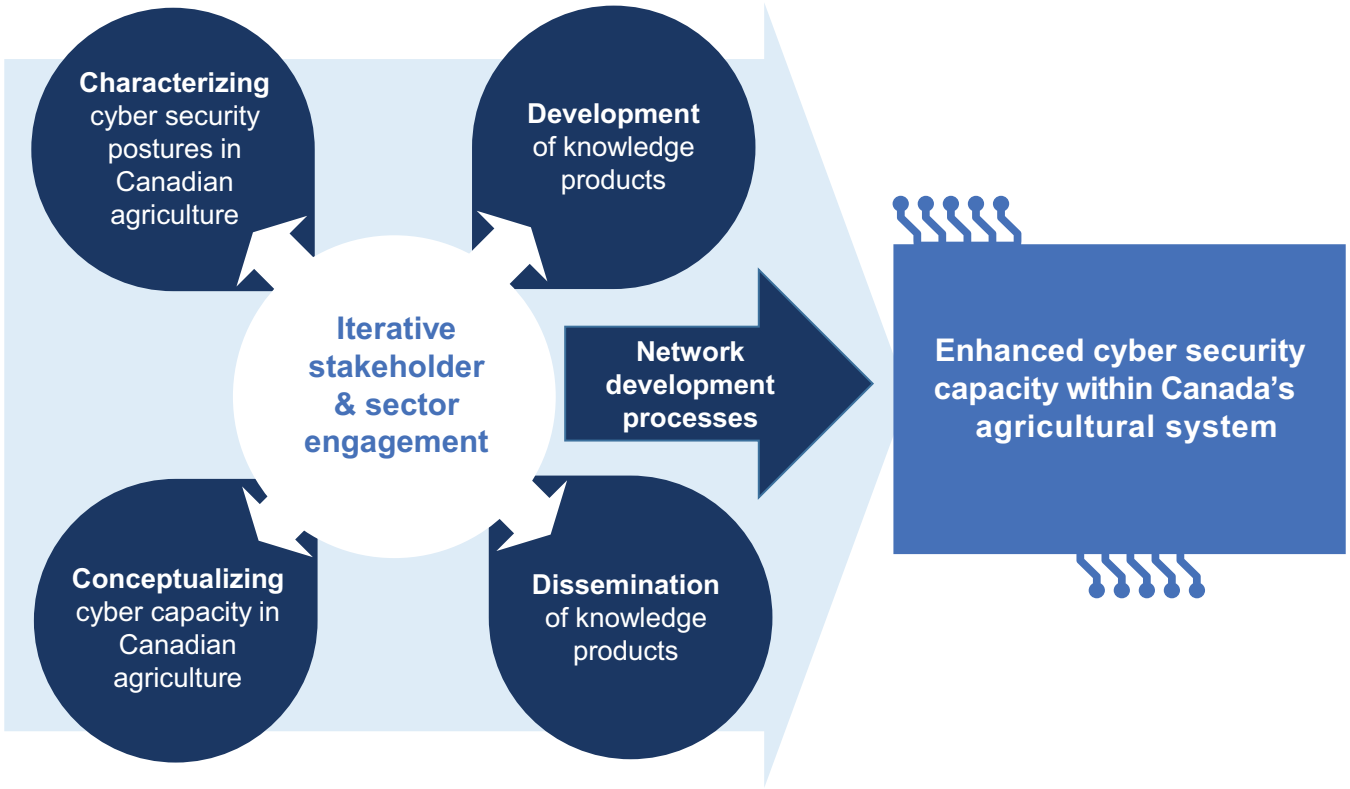
NMR

Schreiber

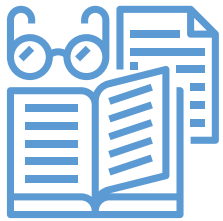
Cyber Security in Canadian Agriculture: Project Overview

Objectives and Outcomes:

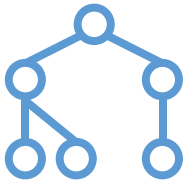
- Characterize current cyber security readiness in the context of evolving threat landscapes.
- Mobilize relevant knowledge across the sector to address threats in practical and effective ways, supporting the evolving cyber knowledge base and enhanced security capacities at the farm/producer level.
- Identify and nurture networked capacity building opportunities for critical infrastructure protection in Canada.



Research and Stakeholder Engagement 2021-22



‘State-of-play’ synthesis of research and policy literature on cyber security in agriculture (domestic and international)



Development of conceptual model – enhancing cyber security capacity in Canadian agriculture

Development of initial cyber risk portfolio matrix

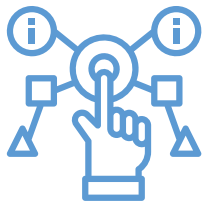
In-depth interviews with industry leaders

In-depth interviews with farm operators

Focus groups with farm operators

National webinars with participant polling

Preliminary, exploratory, producer survey (DEC 2021 –JAN 2022)



Development and distribution print & electronic resources

Media interviews

Podcasts

Converging Learnings To-Date – General Observations

- **Research on digital agriculture cyber-security is still in its infancy**
  - This is both a weakness and an opportunity for accelerated capacity building
  - Recent events (e.g., JBS ransomware) underscore the significance of vulnerabilities
  - Business continuity support, and networked capacity for cyber resilience and defence are lacking
  - Current cyber security protocols have not sufficiently focused on proactive prediction, deterrence, or disruption of attacks or actors

- **Emerging cyber security challenges for Canadian agriculture are to:**
  - Protect the confidentiality, integrity and availability of data, where possible
  - Recognize the risks inherent in interconnected critical infrastructures and supply chains
  - Promote the resilience, prosperity and collaborative capacity of people, supply chains, organizations and communities
  - Defend forward, where feasible

- **The human element** (error and susceptibility to social engineering) is still the most important vulnerability and opportunity for improvement

- **Knowledge mobilization and partnerships** will be essential for building sustainable, capacity to deter, protect, defend, recover – or even transform - operations

Converging Learnings To-Date – Barriers and Vulnerabilities

- **Cyber security is generally not a top priority for farm operators,** most of whom appear to self-manage their IT/IoT networks

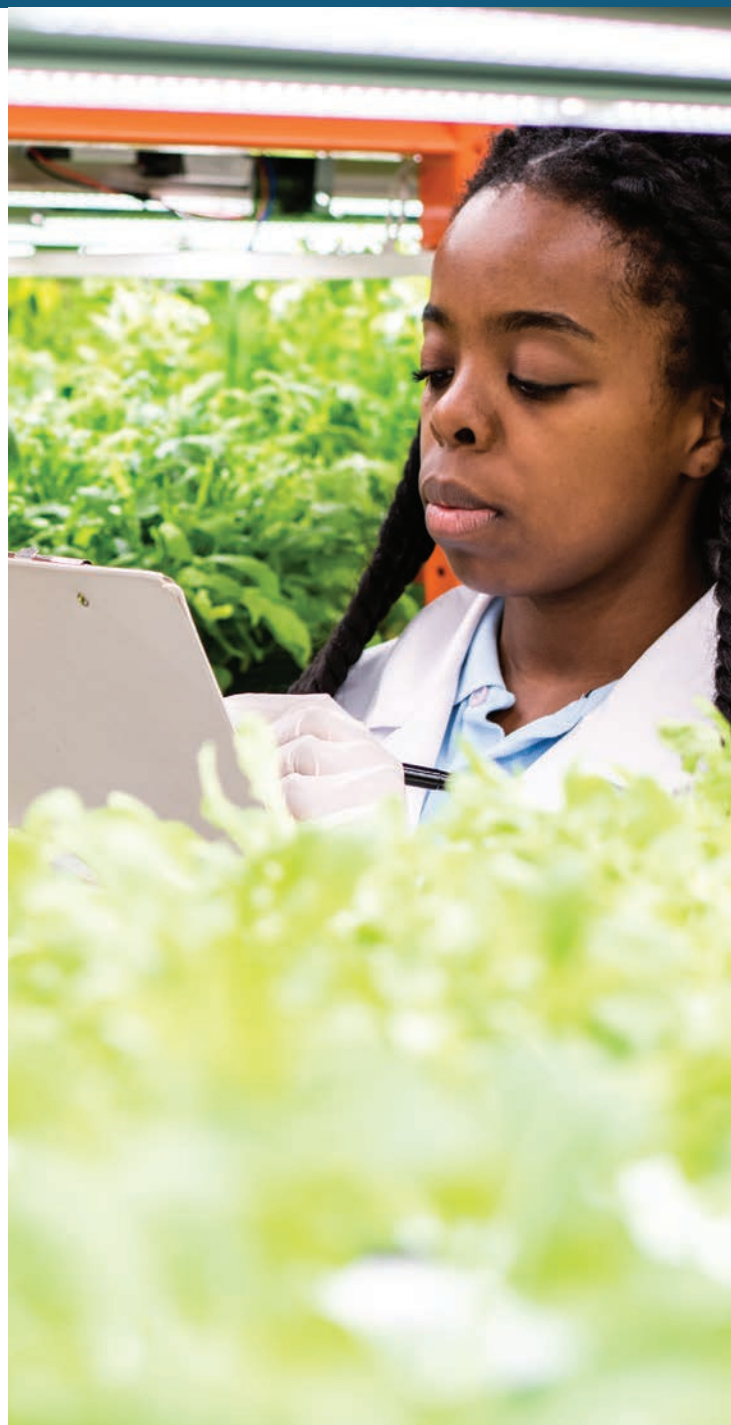
- **Additional barriers among producers to addressing on-farm cyber security include:**
  - **Low perceptions of risk**
  - **Lack of widespread knowledge/cyber situational awareness**
  - **Immature cyber security practices**
  - **Not knowing where to start or where to find resources**
  - **Low investments in cyber security**
    (Average: $541 since January 2020; Range: $0 – $5000)
  - **Major practice changes** are not made as frequently as in other business sectors
  - **Cyber security is not generally seen as a key task, or key part of the identity of farm operators**
  - **Technology hesitancy** tied to privacy and 'right-to-repair' concerns

- **Barriers at other levels of the agfood ecosystem re building cyber security capacity within this critical infrastructure:**
  - Generally not a key priority for commodity sector organizations
  - Cyber security of the agfood sector has not been a high priority across levels of government

Converging Learnings To-Date – Opportunities

- **Digitization is proceeding at pace** –momentum will continue toward 'Ag 4.0'

- **Globally, cyber crime, cyber espionage and cyber warfare are unremitting – these create conditions for change involving:**
  - Building greater awareness and sense of urgency
  - Showing how enhancing cyber security = enhancing business productivity and efficiency
  - Linking producers and their supply chains to resources and tools to make it easy to take the critical basicsteps that will enhance cyber security posture
  - Developing policies and products to develop, strengthen and support networked cyber capacity:
    - Farm-based cyber-hygiene and IoT security
    - Sector-level mutual aid – sharing information and resources, promoting the business case for cyber security, engaging the private and public sectors
    - Public-private partnerships for enhanced cyber security and cyber defence
      - Agricultural cyber security = food security = national security



Directions for Enhancing Cyber Security Capacity

Cyber Risk is Farm Business Risk & Food Security is National Security

Foster farm-level resilience by:
building awareness; addressing business aspirations and concerns of producers; and flowing resources that fit with producer needs

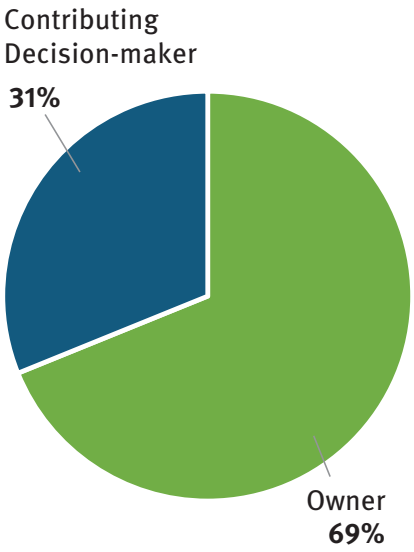
Create processes and partnerships that:
enable networked capacity and mutual aid

CYBER BARN RAISING™

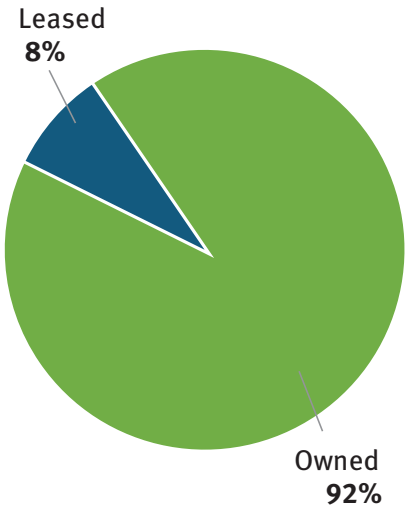
Selected Findings from Preliminary, Exploratory, Producer Survey

- 167 people responded to survey.
- The survey was a self-administered, online survey. Participation was self-selected, voluntary and no compensation was offered.
- This population does not include people who may need assistance with accessing the internet or for whom emails and other social media are not their main source of communication.
- Most respondents run family-owned businesses and three-quarters had more than 20 years experience managing farming operations. A similar proportion of respondents identified as male. The average age of respondents (55-60) was similar to Statistics Canada data.
- The majority of respondents were from ON, AB, SK and MB. They were largely from the following sub-sectors: oilseed and grain; beef cattle; dairy cattle; and poultry and egg.
- Because this exploratory survey was not a random, stratified, sample of Canadian farm operators, findings cannot be generalized to Canadian producers, to specific regions, or to specific sub-sectors. However, preliminary findings bear similarities to findings from the 2021 Australian survey of the agricultural, forestry and fisheries sectors, sponsored by AgriFutures and conducted by BDO, as well as the survey of small businesses conducted by the Canadian Federation of Independent Business in that same year. Our findings point to a number of triangulated themes worthy of further exploration and sector engagement.

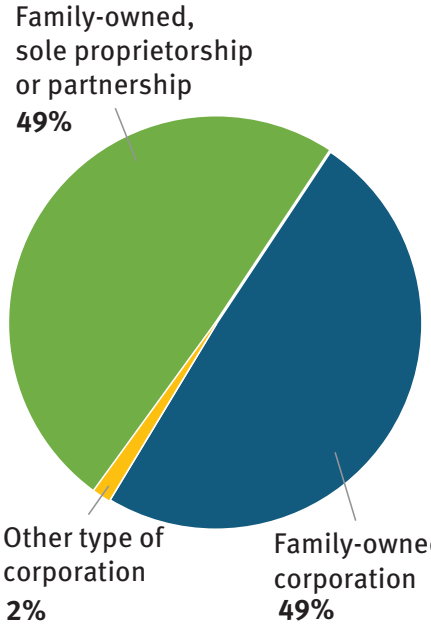
Most of the respondents are the owners of their farm/operation



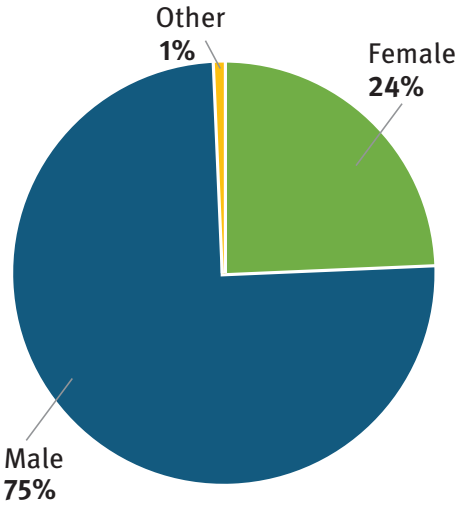
Most respondents own their land



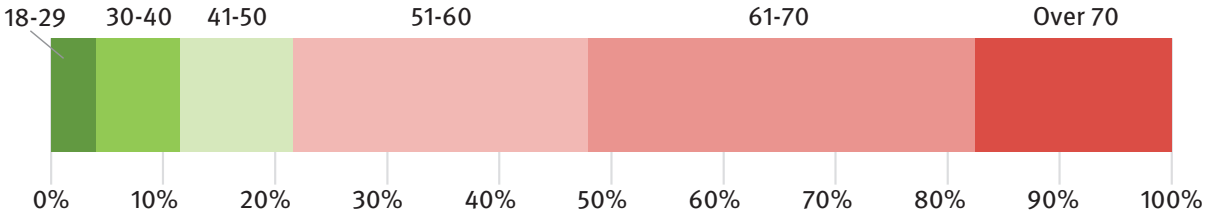
Most respondents run family owned businesses, with half being incorporated



Majority of respondents are male



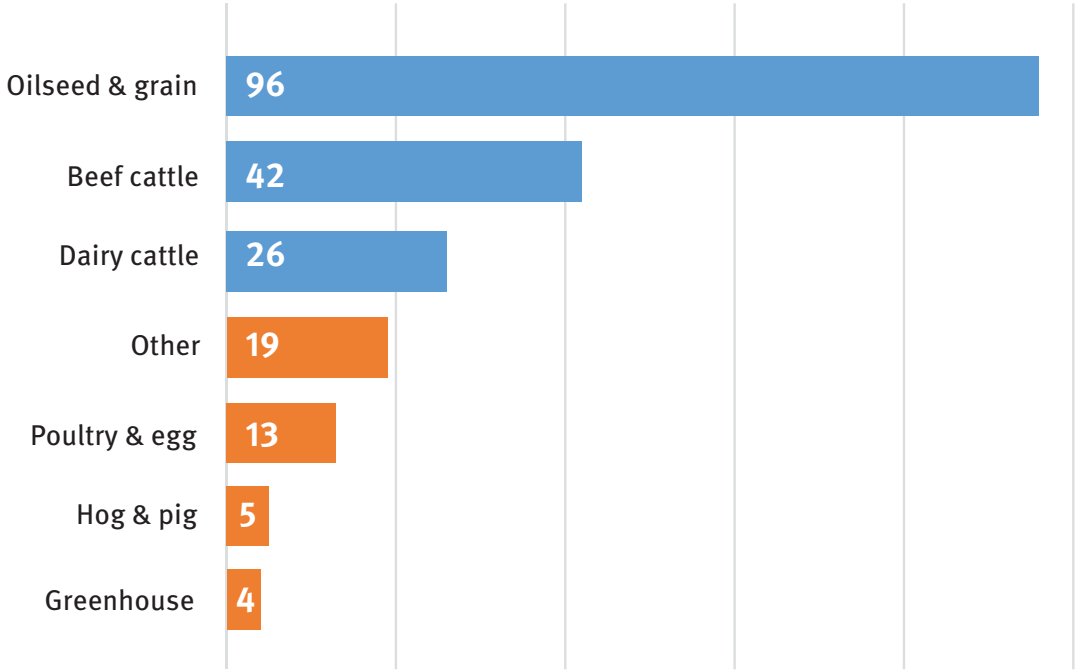
Majority are over 40.
People 40 and younger grew up with internet/technology being ubiquitous



76%
of respondents have more than 20 years of experience managing their farm/ operations

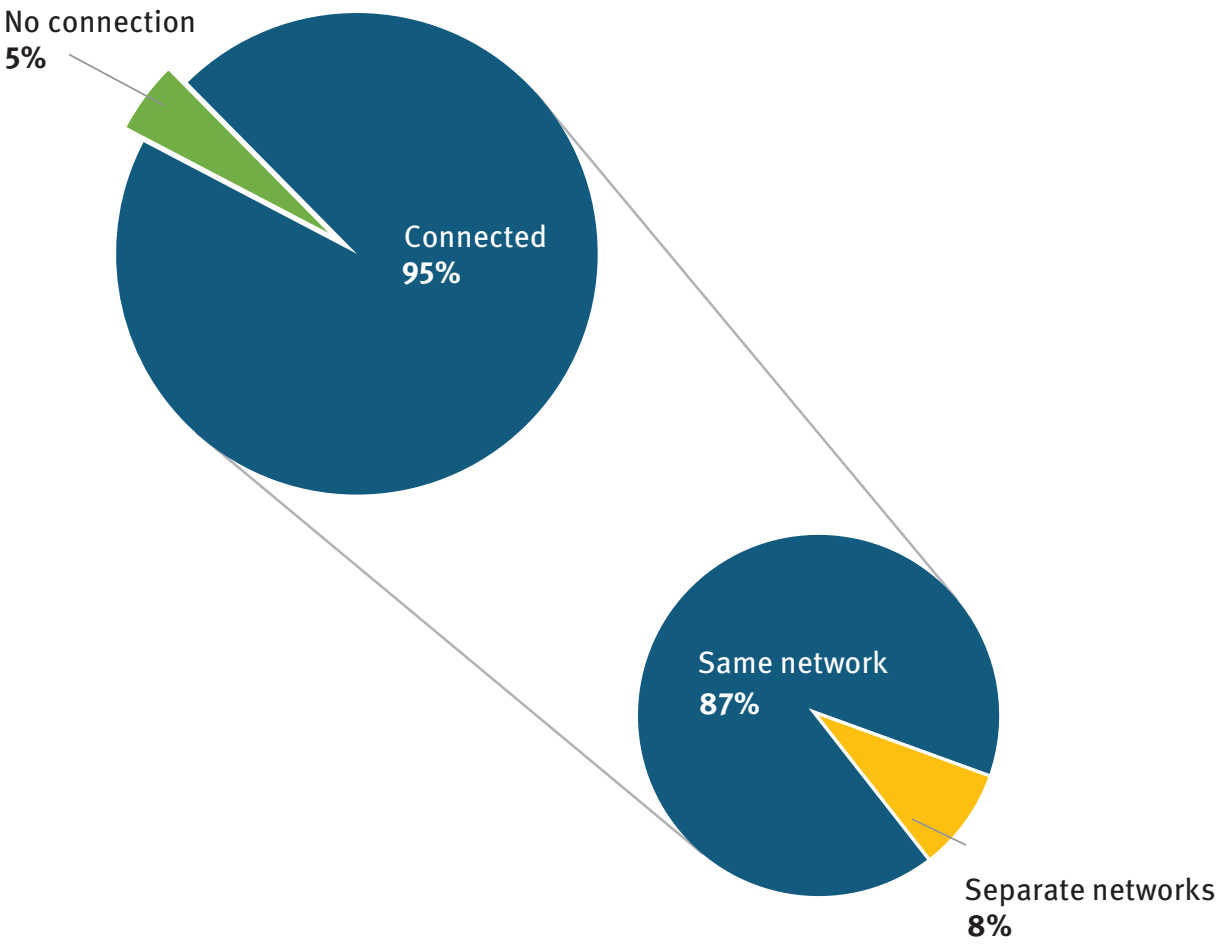
Q8, N=148

Most repondents are from farm oilseed/grain or cattle (beef, dairy)

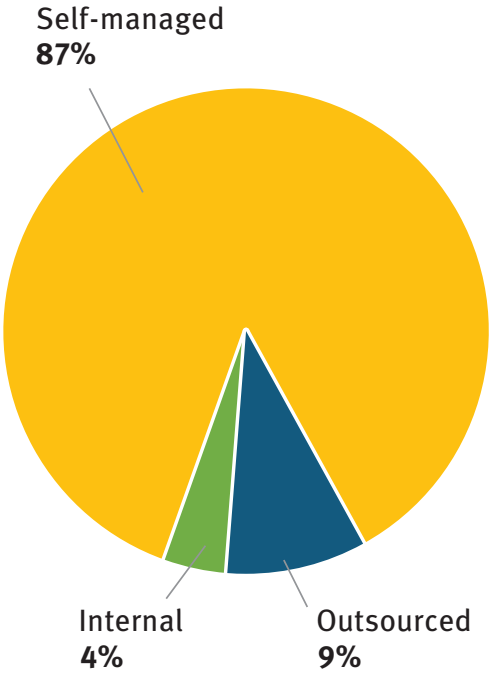


Most respondents have some farm devices connected to the internet or a network.

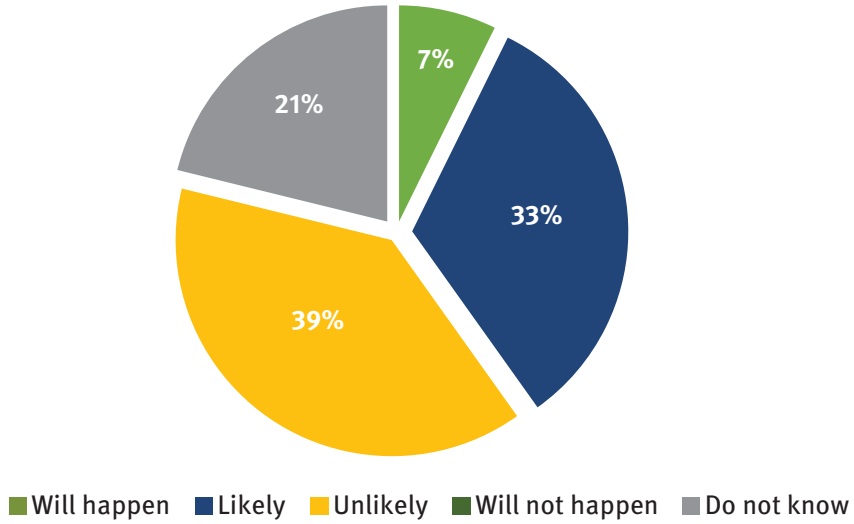
Of those, most use the same network for personal & business.



Of those who are connected, most manage their technology themselves

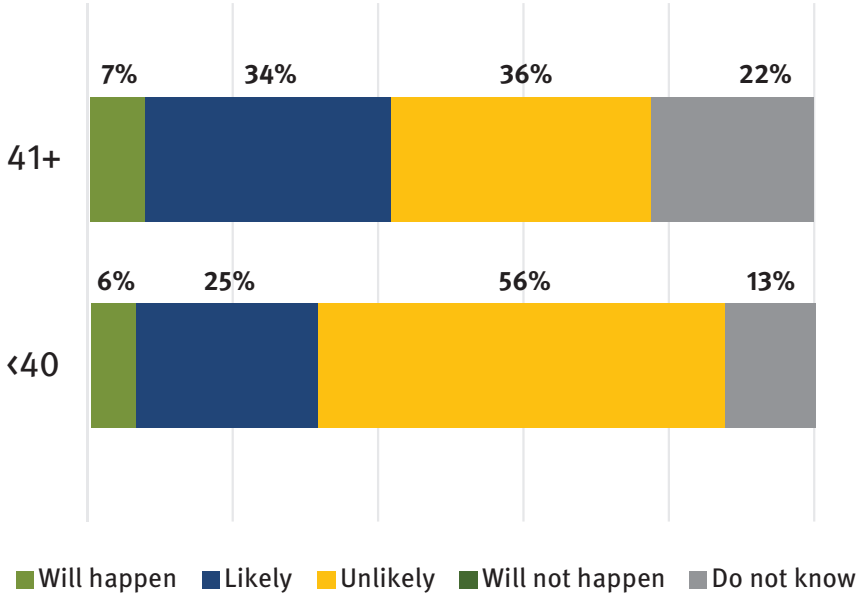


Less than half of respondents thought a cyber security incident will occur



Respondents over 40 were more inclined to think a cyber security incident would occur. More of them weren't sure.

More respondents 40 and under thought cyber security incidents were unlikely.



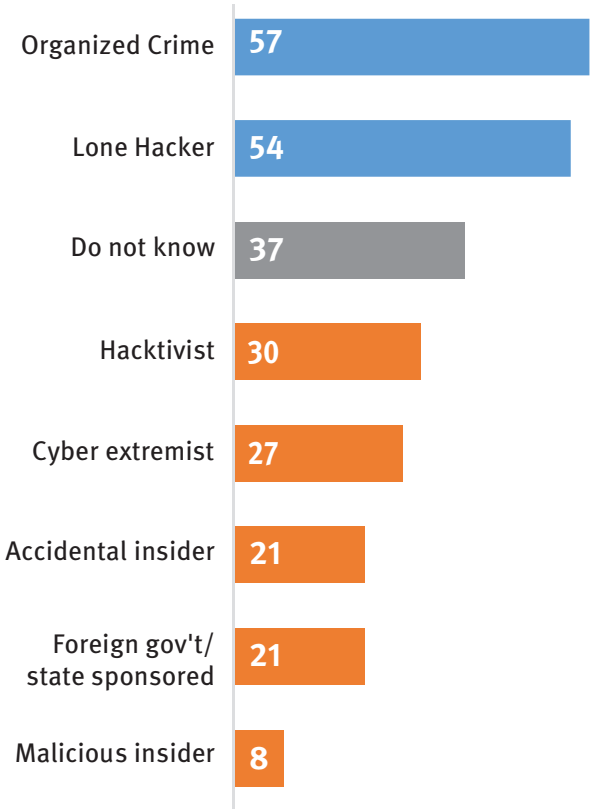
ALMOST 2/3

of respondents were confident that they would be able to manage a cyber security incident on their farm

(29% less confident; 8% don't know)

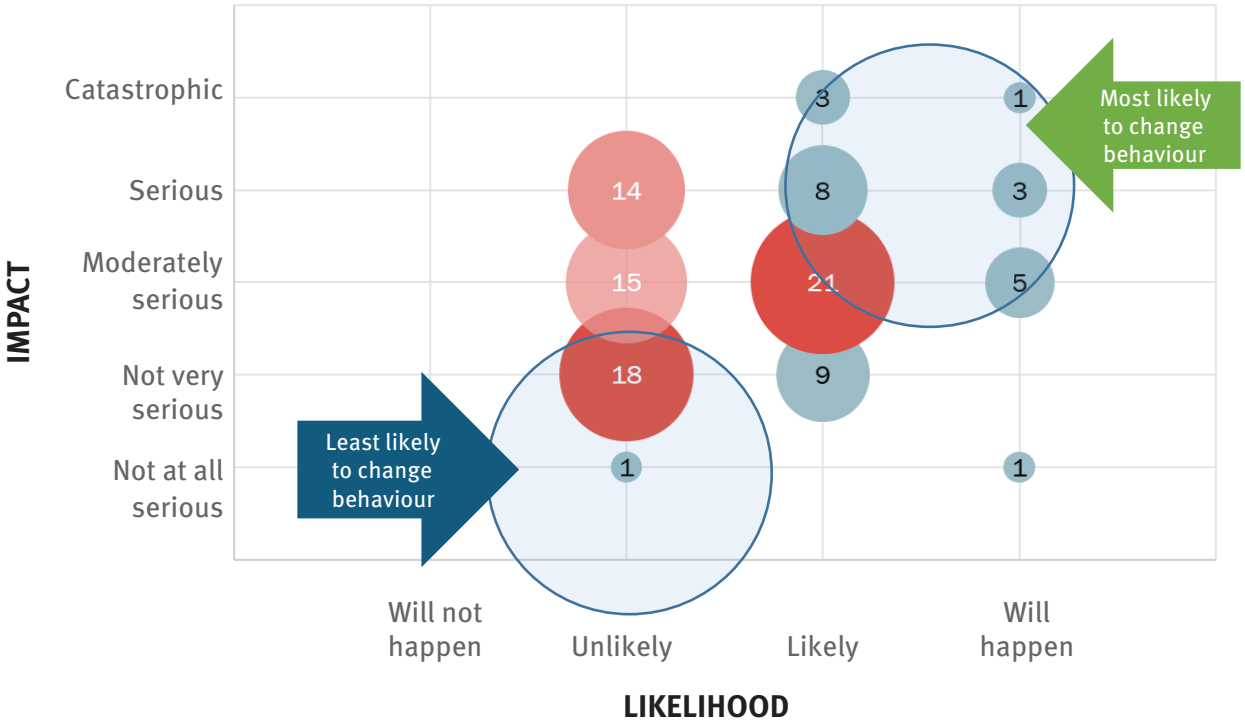
Main sources of perceived cyber threats are individual actors.

Respondents are conscious they are not sure of the threats



Most people perceive cyber security threats as unlikely and not too serious.

Only a few feel that cyber security threats are quite likely and would have serious or catastrophic impacts on their farm operations.

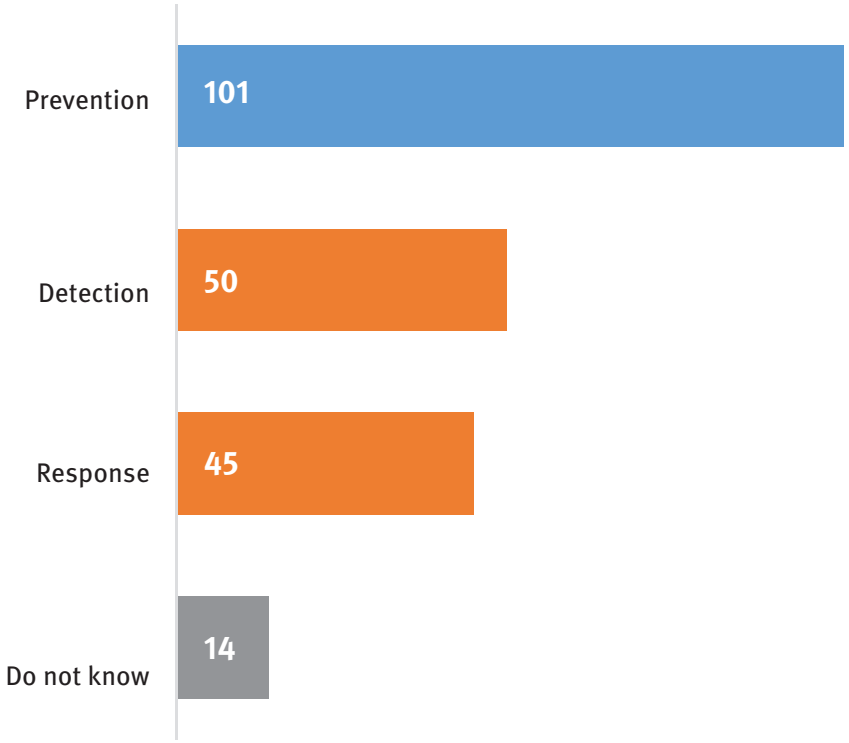


Directing relevant resources and support to those who perceive a threat, and believe it would have serious repercussions for their businesses, can lead to a change in cyber risk management practices.

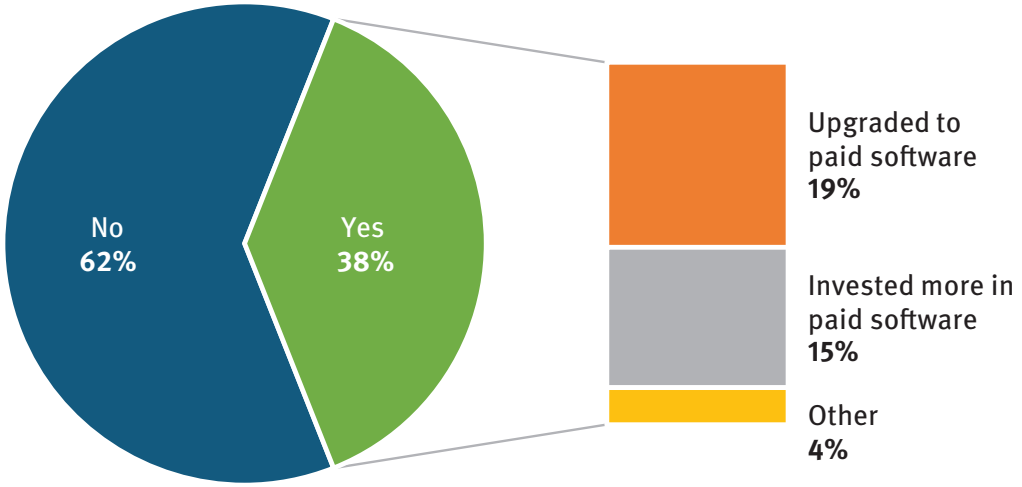
Threats must be seen as manageable from the standpoints of prevention or recovery, and addressing the threats must make business sense.

Inaction can result, not only when people don't perceive a threat as likely and consequential, but also when they feel overwhelmed and don't know what to do or where to turn for help, even when they see a threat as serious and likely to happen.

Prevention is the preferred strategy



Only 38% of respondents invested in new cyber security measures since January 2020



The average amount invested in cyber security made since January 2020 was

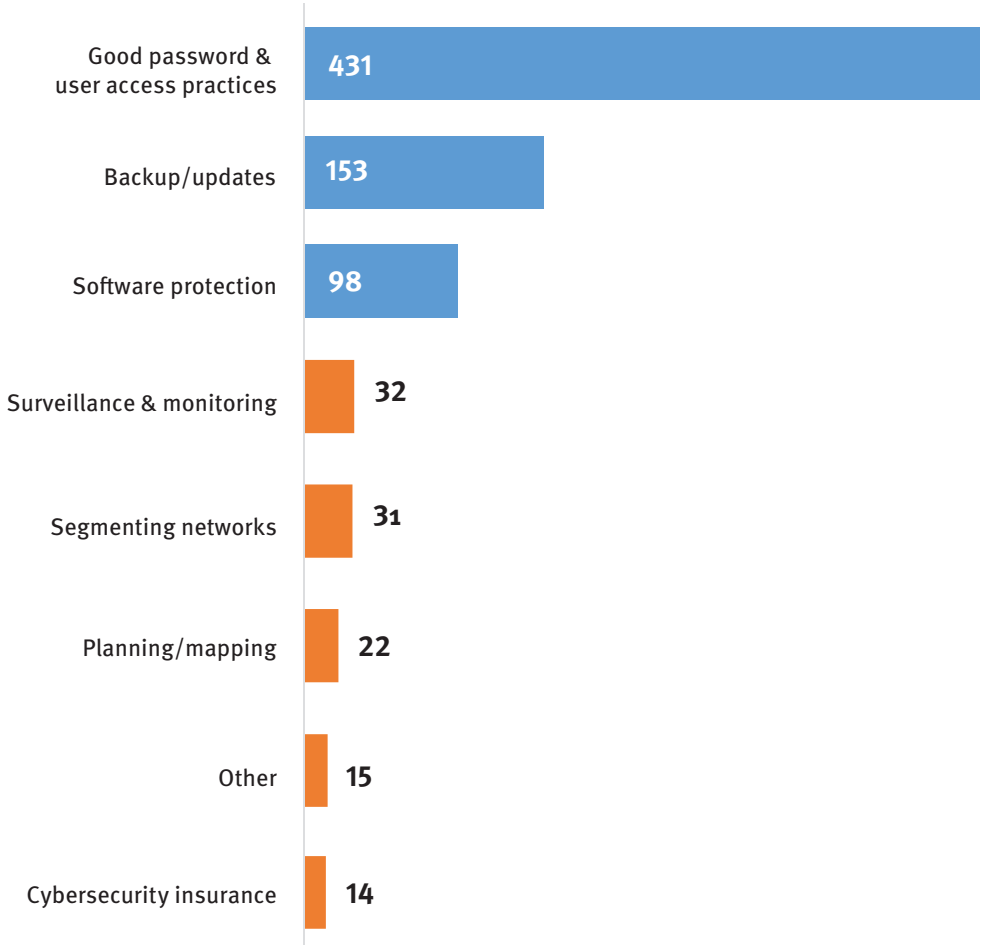
$541

(Median, $100; Range, $0 - $5000)

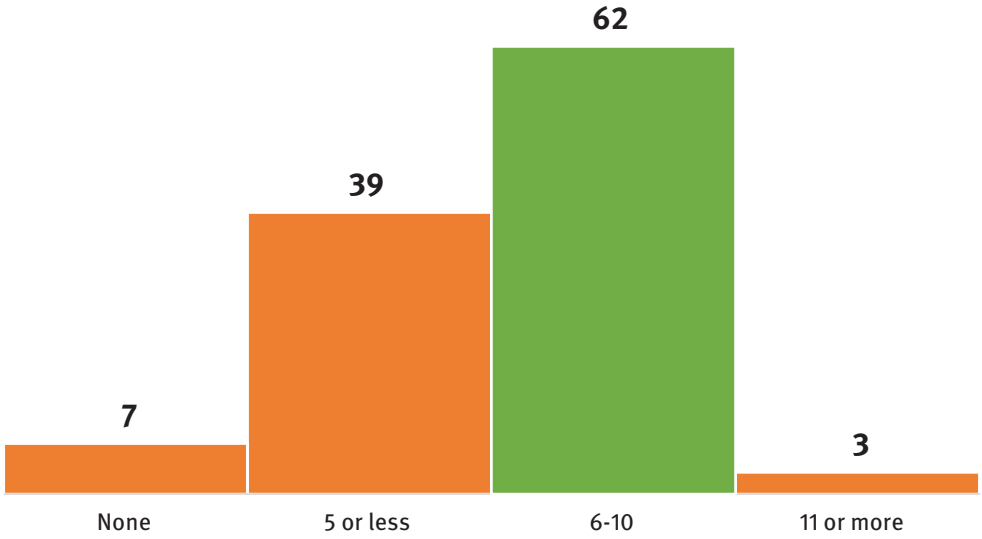
By comparison, CFIB (2021) survey of small businesses estimated that an additional **$6700** was spent on securing IT systems during pandemic

Top practices centre around basic cyber security behaviours.

Assessment, planning and monitoring and advanced behaviours are less practiced



Of 22 identified cybersecurity practices, most respondents were implementing 10 or less.



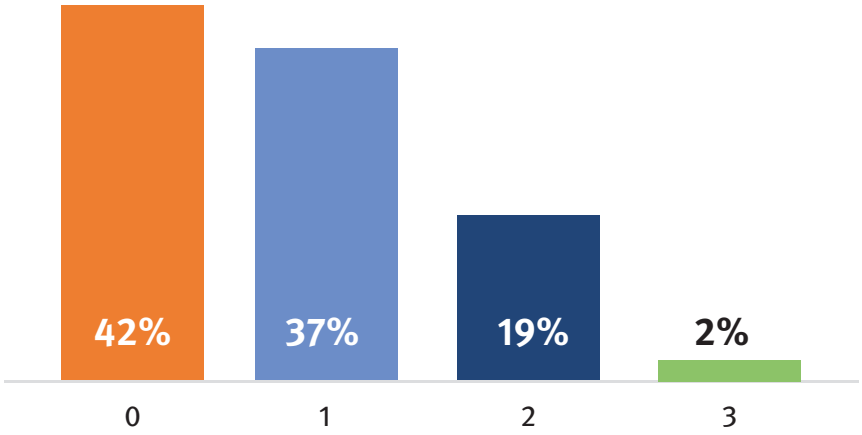
Looking at specific kinds of cyber security practices, most respondents implemented some basic controls, but few had anything approaching a more advanced cyber security program.

Cyber situational awareness was also low:

A good proportion of respondents are receiving information, however most do not practice core cyber security behaviours

42% of respondents are not practicing any of the core cyber security behaviours supporting situational awareness.

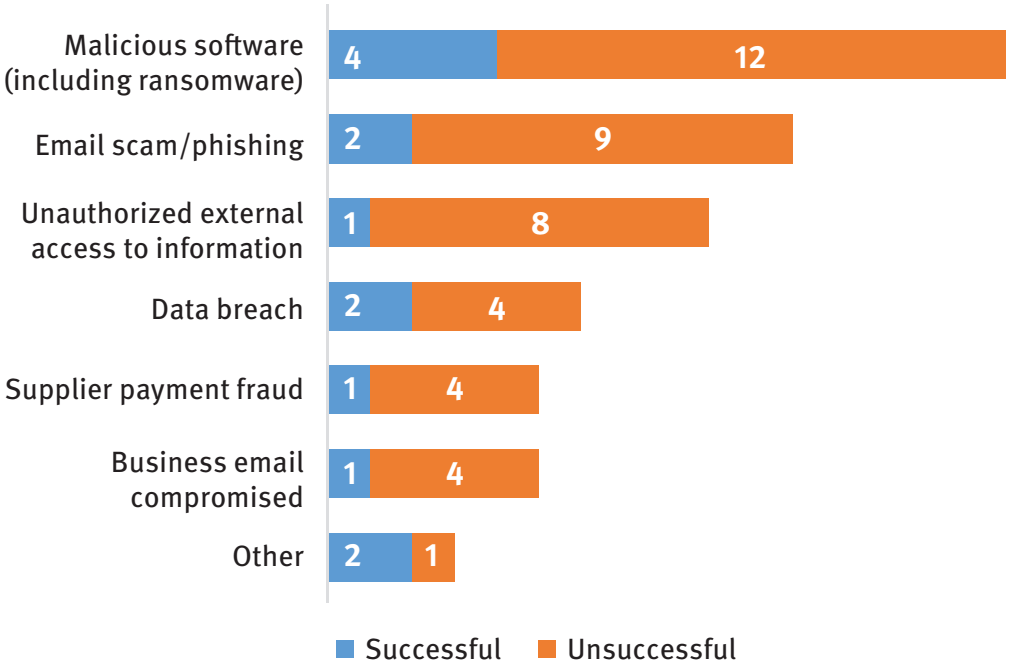
Only 2% are implementing all 3



Among the small number of respondents who reported having experienced some sort of cyber exploit:

All exploits experienced have come from external sources.

The most common of these could be prevented by stronger protection software and awareness

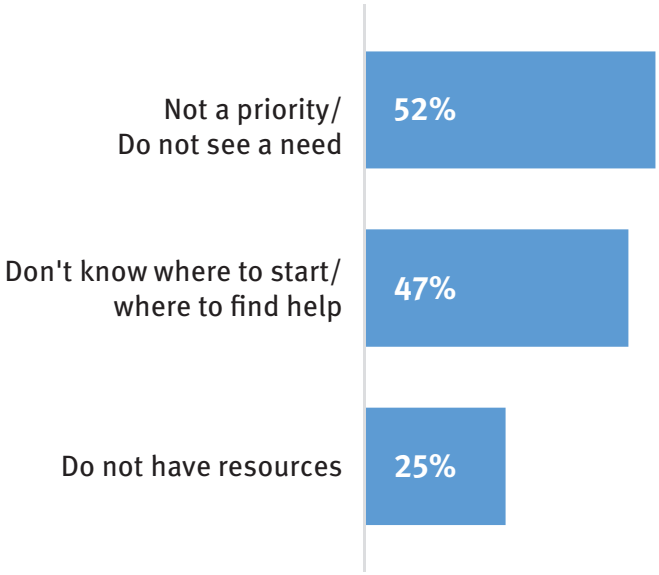


Most respondents are only aware of a cyber security incident after it has occurred

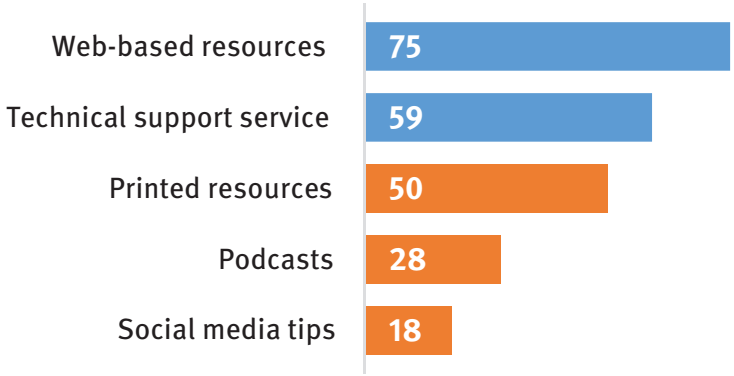
Among respondents who were impacted by successful cyber security incidents:

- Nearly half lost access to information/systems for 1 or more days
- Nearly half required a data recovery process
- Other impacts included: business reputation being damaged, customer records being compromised, intellectual property or trade secrets being stolen, taking down their website

The most significant barrier is that respondents don't know where to start



Most respondents prefer web-based resources for support. A company providing technical support services being the second most preferred

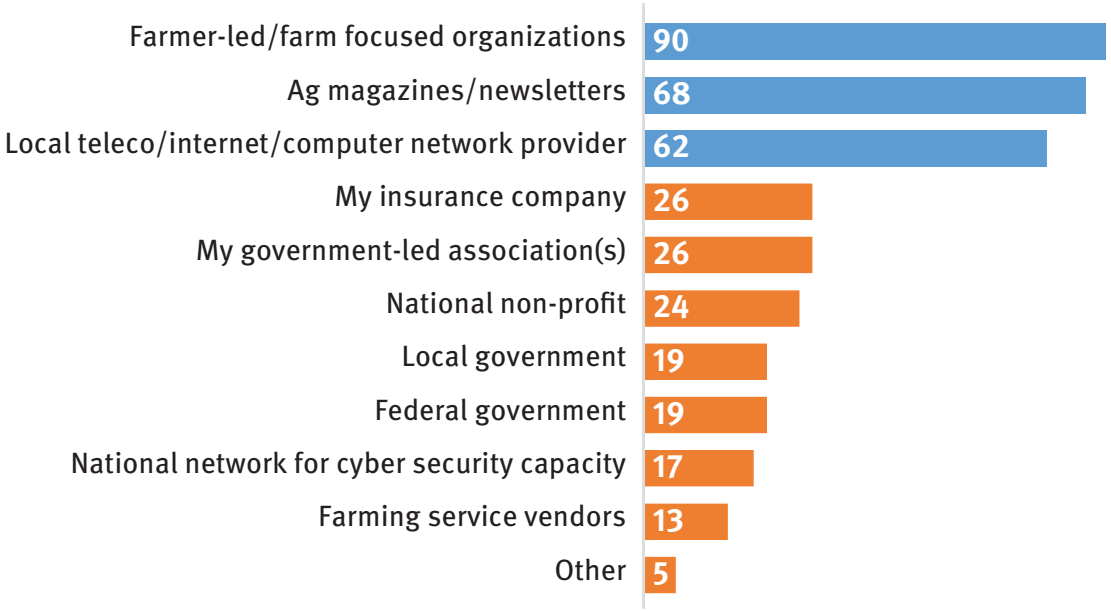


20-25%

of respondents are not seeing cyber security as an issue.

Few see the prospect of a cyber attacks as a realistic or dangerous threat.

Preferred sources of information were through farming organizations, agricultural publications or local internet/network providers



Research Team

Janos Botschner, PhD – Lead

Janos is a social scientist with deep experience in applied research and evaluation and strategic consulting across a range of contexts. He holds a joint doctorate in applied social and developmental psychology. Janos has held a number of adjunct faculty appointments and administrative positions during a lengthy career in the broader public sector. Janos' professional work covers the spectrum of issues related to collaborative public safety and well-being, with a focus on understanding, and responding adaptively to, the complex issues and emerging opportunities of today and tomorrow.

Cal Corley, MBA

Cal is CEO of the Community Safety Knowledge Alliance and a former Assistant Commissioner of the RCMP. Over the course of his career, Cal gained extensive experience in both operations and executive management, serving in such areas as national security, criminal intelligence, drug enforcement, human resources, and leading reform initiatives. He also served on secondments at the Privy Council Office and at Public Safety Canada.

Evan Fraser, PhD

Evan is a full professor of Geography at the University of Guelph and helps lead the *Food from Thought* initiative, which explores how to use big data to reduce agriculture's environmental footprint. As the director of Arrell Food Institute, he co-convened an ad hoc working group made up of producer groups, the food industry, philanthropy and civil society to propose that the Federal Government of Canada should create a National Food Policy Advisory Council. The creation of this council was announced by the Minister of Agriculture and Agri-food Canada in the summer of 2019.

Ritesh Kotak, MBA, JD

Ritesh advises and assists several police services, government bodies, the judiciary, major financial institutions, community partners and private sector organizations with investigations, analytics, principles, practices, challenges and opportunities with respect to the use of social/cyber/digital technology. Ritesh frequently provides interviews to mainstream media to highlight organizational achievements and provide analysis & insights into tech related stories.

Dave McMahon, BEng

Dave's 35-year career has focused on engaged cyber defence, security and intelligence initiatives. Dave was a Special Advisor to the Canadian Security Telecommunications Advisory Committee and expert witness to Senate Standing Committee on Legal and Constitutional Affairs and the National Security and Defence Committees. He has acted in the capacity of a Special Advisor to the Privacy Commissioner of Canada as well as Canadian Intelligence Oversight and Review bodies. Dave serves as Chair of the Cyber Council for the Canadian Association of Defense and Security Industries (CADSI). Dave also served in various leadership positions with the Canadian Armed Forces, Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE).

With additional research contributions from:

Conchobhair Russell, MA

University of Guelph

Elaine Stavnitzky, MSc

Openly

CSKA

Community Safety Knowledge Alliance

Research to Practice to Alignment

The Community Safety Knowledge Alliance (CSKA) is a non-profit corporation that supports governments and others in developing, implementing and assessing new approaches to improving community safety and well-being outcomes.

Janos Botschner
jbotschner@cskacanada.ca

Cal Corley
ccorley@cskacanada.ca

Shannon Fraser-Hansen
sfraserhansen@cskacanada.ca

For further information, visit

www.cskacanada.ca

designed by openly

Certified B Corporation