

STANDARDS RESEARCH

Cybersecurity in the Canadian Food Value Chain

February 2026

Authors

Janos Botschner, Ph.D., Community Safety Knowledge Alliance

Ali Dehghantanha, Ph.D., University of Guelph

Ritesh Kotak, JD, MBA., Ritesh Kotak Consulting; Trupti Enterprises

Dan Lussier, Ph.D., Previously with the Canadian Agri-Food Data Initiative, EMILI

Abbas Yazdinejad, Ph.D., University of Guelph

Cal Corley, MBA., Community Safety Knowledge Alliance

Project Advisory Panel

Adrienne Levay, Lakeland College

Benoit Prévost, Food and Beverage Canada

Brodie Berrigan, Canadian Federation of Agriculture

Darrell Petras, CAAIN

Donald Killorn, PEI Federation of Agriculture

Eric Franke, Ontario Ministry of Food, Agriculture and Agribusiness

Phil Owen, Telus Canada

Steve Rennie, Agriculture and Agri-Food Canada

Nancy Bestic, CSA Group

Rocío Morales Rayas, CSA Group

Don Russell, CSA Group (Project Manager)

Acknowledgements

The authors thank the food value chain parties who participated in the field research component of this work. Their perspectives provided an essential grounding in the lived experiences of people and businesses within this critical infrastructure. We would also like to acknowledge the following individuals who provided feedback on successive versions of this report: Dave McMahon, M.S.M., B.Eng.; Evan Fraser, Ph.D. and Lenore Newman, Ph.D.

Disclaimer

This work has been produced by the authors and is owned by Canadian Standards Association. It is designed to provide general information in regards to the subject matter covered. The views expressed in this publication are those of the authors and study participants. The authors and Canadian Standards Association are not responsible for any loss or damage which might occur as a result of your reliance or use of the content in this publication.

Table of Contents

Executive Summary 6

1. Introduction 7

2 Methods 8

2.1 Literature Review and Environmental Scan 8

2.2 Exploratory Survey of Food Value Chain Actors 9

2.3 Interviews with FVC Actors 9

3 Results and Discussion 10

3.1 Applications of Digital Technologies 10

3.1.1 Wireless and Wired Sensor Networks 11

3.1.2 Automated and Autonomous Equipment and Processes 11

3.1.3 Industrial Control Systems 11

3.1.4 Energy, Waste, and Water Management Systems 12

3.1.5 Decision Support and Quality Monitoring Systems 12

3.1.6 Supply Chain Management and Optimization Systems 13

3.2 Recent Events, Future Hazards, and Emerging Opportunities 13

3.2.1 Technological Cybersecurity Vulnerabilities and Threats 16

3.2.2 Use Case Scenarios 23

3.2.3 Social Cybersecurity Vulnerabilities and Threats 24

3.3 Enhancing Preparedness and Resilience 27

3.4 Jurisdictional Cybersecurity Frameworks and Guidelines 28

3.4.1 Canada 28

3.4.2 United States 32

3.4.3 European Union 33

3.4.4 United Kingdom 34

3.4.5 Netherlands 35

3.4.6 Australia 36

3.4.7 New Zealand 38

3.5 Cybersecurity Standards and Frameworks 39

3.5.1 ISO/IEC 27001, Information Security Management Systems 39

3.5.2 ISO 27701, Privacy Information Management System 40

3.5.3 NIST Cybersecurity Framework 40

3.5.4 ISA/IEC 62443 Series, Automation and Control Systems Cybersecurity Standards 41
3.5.5 IEC 62443-1-5 Technical Specification 41
3.5.6 Office of the Superintendent of Financial Institutions 42
3.5.7 Hazard Analysis Critical Control Points 43
3.5.8 PCI Data Security Standard (DSS), Version 4.0 43
3.5.9 System and Organization Controls (SOC) 2 Reports 44
3.5.10 Control Objectives for Information and Related Technologies (COBIT) 2019 44
3.5.11 Cybersecurity Maturity Model Certification (CMMC) 2.0 44
3.5.12 Internet of Things Security Guidelines (NISTIR 8228, ETSI EN 303 645) 45
3.5.13 Federal Risk and Authorization Management Program (FedRAMP) 45
3.5.14 Center for Internet Security (CIS) Critical Security Controls Version 8 45
3.5.15 Comparison of Standards 46

3.6 Exploratory Survey of Food Value Chain Actors 48
3.6.1 Survey Respondents 48
3.6.1.2 Risk Perception 51
3.6.2 Most Urgent Threats and Vulnerabilities 51
3.6.3 Advancing Cybersecurity and Standards in the Food Value Chain 55
3.6.4 Views on the Potential Role for Cybersecurity and Standards in the Food Value Chain 57
3.6.5 Governance and Leadership in the Development of Cybersecurity Standards for the Food Value Chain 58

3.7 Interviews with Food Value Chain Actors 62
3.7.1 Interview Participants 62
3.7.2 Fragmented Readiness and Growing Digital Risk 64
3.7.3 Sector-Specific Vulnerabilities and Risks 65
3.7.4 Potential Role for Cybersecurity Standardization 66
3.7.5 Enablers and Strategic Levers 67
3.7.6 Governance and Leadership 68

3.8 Key Gaps and Challenges 68

4 Conclusions and Recommendations 74

4.1 Conclusions 74

4.2 Recommendations 78

References 80

Appendix A: Question Guide for Semi-Structured Interviews with FVC Actors 97

List of Abbreviations

AI	Artificial intelligence
CCCS	Canadian Centre for Cyber Security
CCPs	Critical control points
CI	Critical infrastructure
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CRG	Cyber Security Readiness Goals
CSKA	Community Safety Knowledge Alliance
ETSI	European Telecommunications Standards Institute
FVC	Food value chain
GDPR	General Data Protection Regulation
HACCP	Hazard Analysis Critical Control Points
IACS	Industrial automation and control systems
ICS	Industrial control systems
IEC	International Electrotechnical Commission
IoT	Internet of things
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
IT	Information technology
NIST	National Institute of Standards and Technology
OSFI	Office of the Superintendent of Financial Institutions
OSI	Open Systems Interconnection
OT	Operational technology
RFID	Radio frequency identification
SCADA	Supervisory control and data acquisition
SMEs	Small and medium enterprises

Executive Summary

Canada's food system is undergoing rapid digital transformation, creating a generational opportunity for sectoral growth. However, this transformation also creates new categories of risk related to comparatively underdeveloped cybersecurity. The food system is one of Canada's ten critical infrastructure (CI) sectors, and any heightened risk to this system must be addressed. This CI is particularly vulnerable to cyberattacks due to its interconnected nature, which links it closely with other sectors, such as energy, transportation, telecommunications, financial services, and healthcare. Recent cyber incidents, including ransomware attacks against major food processors, agricultural cooperatives, and grocery retailers, underscore the urgency of addressing cybersecurity risks across the food value chain (FVC). The cybersecurity of Canada's FVC is essential not only for economic resilience and public safety but also for national security. This research report improves understanding of the evolving cybersecurity landscape of Canada's FVC; identifies key vulnerabilities and threats; and explores policy, regulatory, and standardization considerations related to cybersecurity preparedness and resilience. The research included:

- A literature review and environmental scan of academic research, cybersecurity standards and guidelines, and jurisdictional policies and strategies relevant to the FVC;
- An exploratory online survey of relevant Canadian FVC parties to develop a preliminary understanding about the perceptions of cybersecurity awareness and risks, and views on standards; and
- Interviews with Canadian FVC experts and interested parties to deepen understanding of views on sector-specific cybersecurity threats, vulnerabilities, and opportunities related to standardization.

Despite the importance of food system cybersecurity, the sector lags other industries on this topic. There is scant peer-reviewed research or standards literature on cybersecurity in the food system, and the topic is largely absent from cybersecurity policies and frameworks. Existing cybersecurity standards and strategies adopted by other countries may offer valuable guidance, but lack specificity for the unique operational, technological, and environmental contexts in Canada. Engagement with relevant interested parties from the FVC revealed that adoption of digital technologies within the sector is progressing, but understanding of cybersecurity risks is not keeping pace with the level of adoption which may constitute a barrier to adoption. While research participants highlighted what they saw as pressing threats (ransomware, data breaches, phishing, and potential cyberterrorism) and important vulnerabilities (limited employee training and weak cyber hygiene and organizational governance), they viewed their peers as less aware and less seized by these issues. There appears to be support for a degree of Canada-specific standardization within the FVC, based on multi-party collaboration, involving traditional and non-traditional actors, reinforced by awareness building, training, and guidance via trusted channels, support and incentives, and governance. This important opportunity for capacity building could be achieved by:

- Establishing a cybersecurity standardization criteria for the Canadian agri-food sector, involving a diverse cross-section of actors;
- Deploying a novel set of principles to guide cybersecurity standardization in the FVC; and
- Implementing governance that involves centralized oversight with decentralized implementation. This would enable strategic direction and accountability, and integrated policy development, while sector-specific and regional working groups would help ensure localized relevance, supporting practical, achievable implementation and broad engagement.



"Canada's food system is in the midst of a transformation underpinned by digital technologies."

1. Introduction

Canada's food system is in the midst of a transformation underpinned by digital technologies. Services and equipment, such as platforms providing enhanced access to analytics or tie-ins to supply chain components, along with industrial control systems, low-cost sensors, actuators, autonomous machinery, and GPS-enabled equipment, are driving unparalleled opportunities for productivity, efficiency, and sustainability across the agri-food value chain (FVC), from primary production to processing, distribution, and retail. Despite their potential benefits, these technologies also entail socio-political challenges [1] along with risks to the digital systems that are increasingly the lifeblood of this critical infrastructure (CI), which the Government of Canada defines as: [the] *processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. CI can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of CI could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence* [2].

The National Cross Sector Forum 2021–2023 Action Plan for Critical Infrastructure identifies the food system as one of ten CI sectors in Canada [3] (although food is identified, it is not defined).

The other sectors are energy and utilities, finance, transportation, government, information and communication technology, health, water, safety, and manufacturing. The National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure (2021) [4] is to be implemented to achieve and enhance CI resilience according to three strategic objectives:

- Building partnerships;
- Sharing and protecting information; and
- Implementing an all-hazards approach to risk management.

Due to its position at the intersection of multiple supply chains and other sectors (e.g., energy, telecommunications, water and wastewater, transportation, financial services, and animal and human health), the broader food system—particularly the FVC—is also a component of a network of interdependent CIs [5] (i.e., the food system intersects with the other nine CI sectors). These relationships are shown in Figure 1. The food CI, and the FVC in particular, are vulnerable due to their underdeveloped cybersecurity compared to other sectors of the Canadian economy [1], [5], [6], and a digital divide between smaller and larger FVC businesses, such as farming operations [7]. This means that an essential component of Canada's domestic prosperity and well-being, and its geopolitical role as a major food exporter, are at risk of being compromised by intentional or inadvertent actions that impact data

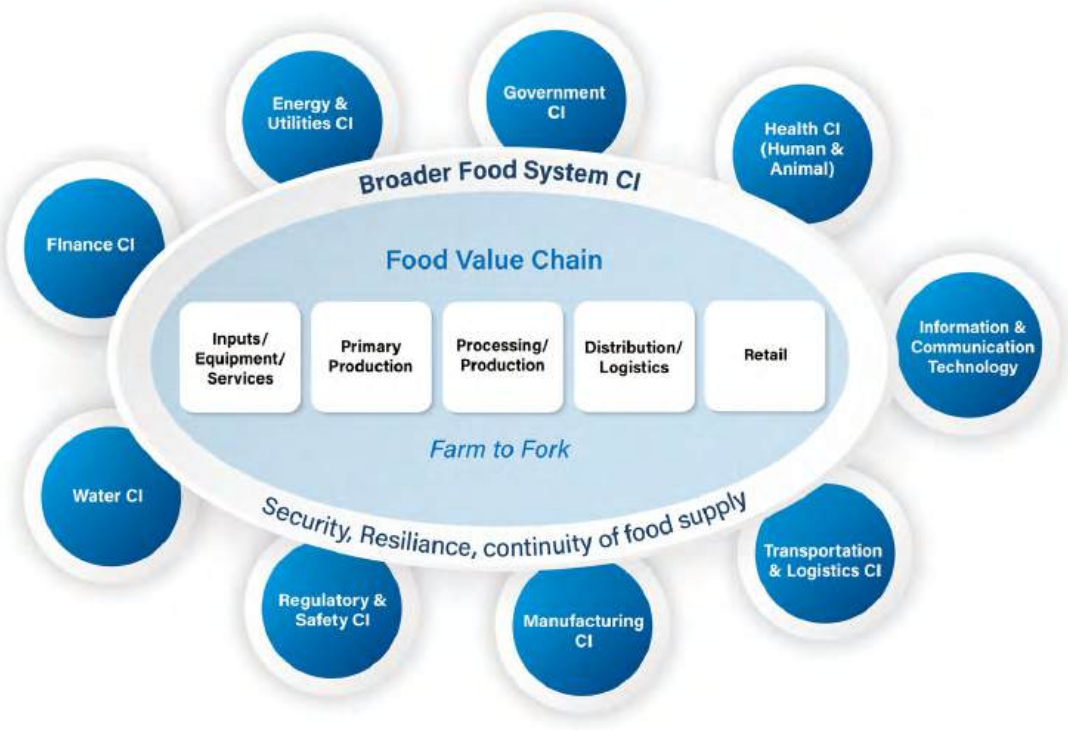
confidentiality, integrity, and availability [8]. The need for greater focus on cybersecurity across the FVC is not unique to Canada [9], [10]. Focus on this topic within published English-language literature, policies, and standards is limited. Research on the human side of cybersecurity suggests that a portfolio of actions might remediate current vulnerabilities and place Canada's food system on a more cybersecure and resilient footing. These actions are encompassed within a sector-specific cybersecurity framework [11] that works across multiple domains. Successfully dealing with the threat landscape of digitally integrated flows of goods and services will require strategic mixes of technological and human-centric approaches, in addition to effective policy and regulatory measures [12]. Prioritizing attention to standards and human-centred design principles [13] is crucial to fostering a security culture that can readily adapt to the constantly evolving threat landscape. The objective of this report, therefore, is to understand the cybersecurity landscape of the Canadian FVC, including current and emerging cybersecurity challenges associated with technology trends, and relevant policy, regulatory, and standardization dimensions that support cybersecurity and cyber resilience.

2 Methods

2.1 Literature Review and Environmental Scan

The literature began review by integrating work conducted by Rotz *et al.* [1], Botschner *et al.* [5], [6], [8], [11], [14], [15], and Yazdinejad *et al.* [13], [16], [17], [18], [19], which emphasized cybersecurity in the agricultural production component of the FVC, which was the starting point for attention to food system cybersecurity from 2016 to 2023. This was followed by work to develop an understanding of the attention paid to cybersecurity standards relevant to the FVC. An evidence synthesis was conducted, drawing from systematic review and snowball sampling methods [20]. The following search terms were entered into

Figure 1: The FVC, within the food system critical infrastructure (CI), sits at the intersection of the other CIs identified in the National Strategy for Critical Infrastructure (adapted from [3]).



the Google Scholar search engine: "cybersecurity standards" OR "cyber security standards" AND "food system" OR "food value chain" OR "agri-food chain"; and "cybersecurity standards in the food value chain". The search period was 2020–2024. Articles were screened for eligibility based on at least some attention (in the title or the abstract) to cybersecurity related to either the FVC as a whole, or to specific components of the FVC or key FVC technologies (e.g., agriculture, processing, supply chains, advanced manufacturing). In terms of policy, regulatory, and compliance documents, an environmental scan was conducted of available English-language cybersecurity-focused policies and frameworks from six western democratic jurisdictions with expanding digital food systems and a NATO member state. A review of cybersecurity standards and guidelines was also conducted. The review of government and government-supported cybersecurity-focused policies, legislation, and supports focused on Canada, the United States (US), the United Kingdom (UK), Australia, New Zealand, and the Netherlands. The objectives were: (a) to understand the nature and variety of cybersecurity responses in place or under development; (b) to characterize the depth and breadth of focus of these responses; and (c) to attempt to discern how cybersecurity within the FVC was represented, if at all.

2.2 Exploratory Survey of Food Value Chain Actors

A confidential self-report online survey was created to explore the views of relevant FVC parties about cybersecurity across the sector and the potential role that Canadian sector-specific standards might play in strengthening cybersecurity across the FVC. The survey was structured to probe different levels of knowledge and experience with cybersecurity and was designed to take between 10 and 15 minutes to complete. English and French versions of the survey were created, each with their own links. These were actively promoted to relevant parties, including manufacturers, farmers, associations, and other FVC actors. The surveys, which were hosted on the Survey Monkey platform, were advertised in December 2024, then more actively promoted through direct (email and sector conference presentations) and indirect (LinkedIn) channels from January to March 2025.

2.3 Interviews with FVC Actors

To deepen understanding of cybersecurity perspectives within the FVC and explore how standards might enhance cyber preparedness and resilience, a series of semi-structured conversational interviews was conducted over videoconferencing. Participants were drawn from a purposive [21] sample designed to be as rich and relevant as possible in terms of FVC knowledge and experience (i.e., that covered relevant categories from the FVC and included individuals with a depth of industry knowledge and experience). Prospective interviewees were invited to participate via email. Prior to the interview, they were provided with background information on the project's objectives and the specific topics to be discussed during the interview. The interview guide is included in Appendix A. Interviews were conducted over Zoom or MS Teams and ranged from approximately 30 to 60 minutes. At the outset of each interview, participants were reminded of the purpose of the conversation and were informed that the interview would be confidential (i.e., comments would not be attributed to specific individuals in the published report). They were provided with opportunities to ask questions and the request for consent included that the interview was to be audio-recorded. All participants provided consent for the interviews to proceed as described. Individual interview transcripts were reviewed to generate a provisional list of key themes, and then a thematic analysis was conducted at the group level to identify key insights and implications related to the focus of the project. Multiple passes were made through the interview transcripts to re-check and confirm saturation [22] of the identified themes. Insights from the survey and interview components were considered together in discussing the implications of the findings for enhancing cybersecurity within and across the FVC.

3 Results and Discussion

The Canadian FVC is comprised of numerous industries, including:

- Primary agriculture and aquaculture;
- Food and beverage processing;
- Food services;
- Food retail and wholesale; and
- A range of input (animal feed, fertilizers) and service suppliers (business and farm advisors, data analytic services, technology vendors and services, and telecommunications providers).

Together, these represent a network with the primary aim of enhancing the profitability of each participant by building a sustainable competitive advantage [23]. Previously, a distinction was made between value chains and supply chains. Broadly speaking, the former focused on value creation within organizations (e.g., [24]), while the latter focused on the successive flows of information and materials from one segment of a chain to another [25], from the sourcing of raw materials to the delivery of the final product [26]. However, with increasing inter-connections between organizations and a range of third parties (e.g., through outsourcing of critical operational functions), this distinction is becoming less relevant. For the purposed of this report, the terms FVC and supply chain are considered to be interchangeable.

3.1 Applications of Digital Technologies

Canada has an active innovation ecosystem for agri-food technologies. In agriculture, examples of innovative digital technologies include robotic mushroom picking systems [27], the use of robotic and spectroscopic technologies in fruit orchards [28], and an emerging network of "smart farms" test sites designed to support technology incubation and demonstration as well as being an adjunct to education and training [29], [30]. In food processing, distribution, and retail, digital technologies are being used to enhance the efficiency of each of these FVC components, including automated sorting, slicing, cleaning and packing; quality monitoring (e.g., temperature ranges); transportation route planning and tracking; energy management and optimization; and the use of radio frequency identification (RFID) systems and imaging for inventory control [31]. Furthermore, the deployment of artificial intelligence (AI) in the agri-food system is expanding opportunities to integrate robotic and sensor-based technologies in the FVC. AI and digital ecosystems as being promoted as catalysts for sustainable, data-driven food and agricultural systems focusing on efficiency, safety, and quality [9], [10]. Enhanced use of data in these parts of the agri-food sector create opportunities to improve food safety and traceability, which is an area of increasing consumer interest and an important aspect of international trade, as mandated in many jurisdictions. For example, the European Union (EU) General Food Law (Regulation EC No 178/2002) mandates that all food and feed products be traceable throughout the entire FVC [32]. In Canada, the Canadian Food Inspection Agency describes food safety as a shared responsibility and an outcome of collaboration and continuous improvement, incorporating technological innovation for safety management [33]. Despite the growing use of digital technologies within the agri-food sector, their level of adoption is limited compared to other CIs and sectors, such as energy, financial services, and manufacturing. Some have suggested that this reflects supply chain variability and maturity factors [34]. Taken together, the digital components of the FVC can be seen as a comprehensive "bundle" of technologies designed to optimize agricultural production and food processing, improve the distribution of agricultural commodities and value-added products, and streamline the commercialization of food products [35]. At one time, all of these were emergent innovations. Today, many combine features that can be regarded as common "enabling" digital technologies (e.g., industrial control systems) with innovative features, such as wireless sensors [35] or blockchain technologies for smart contracting [36]. Generally, the bundle of digital food system elements can be characterized by several overarching groups of technologies [5], which are discussed in sections 3.1.1 through 3.1.6.



3.1.1 Wireless and Wired Sensor Networks

Sensor networks use hardware endpoints to measure and transmit data about a wide range of conditions, such as soil temperature and moisture levels, environmental air temperature and physical properties, visual features of crop lands, livestock health and behaviour, water and waste levels, and indoor environmental conditions [37], as well as moisture levels and food safety considerations in processing. Data from sensor networks can be integrated into other production and processing systems, providing real-time information across various operational dimensions, including yield, livestock activity and wellbeing, livestock barn and greenhouse environmental monitoring, biosecurity and public health surveillance, water management, fertilizer and pest management, frost prediction, and inventory and asset tracking (e.g., supply levels, tractor and irrigation system movements) [34], [38].

3.1.2 Automated and Autonomous Equipment and Processes

Digital automated equipment is becoming more common [39], [40] and includes advanced implements, irrigation systems, and robotics in food processing. For example, in the dairy industry, automated milking parlours reduce labour requirements while simultaneously enhancing animal health through the use of sensor technology and providing important insights into production [41], [42]. Autonomous agricultural equipment is expected to revolutionize the sector. For example, GPS-enabled planting and harvesting systems can drive increases in efficiency and accuracy, and emerging technologies that combine unmanned aerial vehicles with robotics and AI are promising to advance crop monitoring, as well as pest and weed control. Furthermore, various combinations of automated and autonomous machinery and robotics are being used in food processing, including meat processing assemblies, roasting and grinding, packaging, and warehousing and loading. Autonomous technology requires significantly more computing resources and network capability; it also places demands on users to upskill in order to safely and effectively deploy these technologies. For example, telerobotics blend sophisticated technologies with remotely located human operators. This additional complexity means that these systems also entail more cyber risks [43].

3.1.3 Industrial Control Systems

Industrial control systems (ICS) manage devices to regulate operational processes, ranging from basic heating, ventilation, and air conditioning to large distributed systems with multiple connections and endpoints in complex industrial facilities. These larger systems, often known as SCADA (supervisory

control and data acquisition) systems, consist of various connected devices, controllers, and graphical user interfaces that enable autonomous or semi-autonomous monitoring and regulation of complex processes. In agriculture, ICS/SCADA systems are used to monitor, automate, and optimize irrigation and the application of materials (such as fertilizers and irrigation), and to autonomously regulate indoor growth or storage conditions for agricultural commodities and facilitate harvesting some agricultural items [44]. While other digital production technologies (e.g., farm equipment, weather stations) are not SCADA systems per se, they are no less vulnerable to malicious cyber exploits. In food processing, ICS/SCADA systems help to ensure that a variety of key functions are maintained within appropriate limits of safety, efficiency and quality [45]. In warehousing and retail, integrated inventory control, enterprise resource planning systems, purchasing and logistics systems also help to optimize input and output control [46]. This can contribute to lower costs, lower emissions, and fewer delays for downstream customers. Over time, industrial control systems have evolved from being separate, standalone networks to highly connected and complex systems. As separate networks, these systems were naturally protected from most cyberattacks. The growth in connectivity to various business networks and cloud services has increased the vulnerability of these systems to cyberattacks by expanding the number of potential attack surfaces [47]. The consequences of disrupting ICS/SCADA systems in the FVC can include too much or too little irrigation, leading to crop losses; processing food at temperatures outside of control limits, impacting food safety; or allowing internal growing environments to surpass optimal temperatures, which may lead to reduced outputs. When this involves environmental control systems within livestock barns, this could also lead to animal welfare emergencies, including deaths, in some cases.

3.1.4 Energy, Waste, and Water Management Systems

Effective waste management or water treatment systems are essential, not just for individual farming operations but also for the surrounding environment and connected systems. Poorly controlled waste management or water treatment systems may compromise animal or human health at various points along the supply chain [48]. Renewable and low-carbon energy options are growing in importance in both food processing and farm operations, and technological development is on a fast-track. Statistics Canada reported that between 2015 and 2021, the rate of renewable energy production on farms doubled [49]. On-farm energy management systems with cyber-physical components include photovoltaic microgrids, geothermal and wind energy systems, waste heat recovery systems, and biofuel and biomass combustion. Some farms make use of mixed energy generation systems, known as cogeneration or multigeneration systems [50], which may serve a variety of functions [51] and have been identified as a leading technology for reducing greenhouse gas emissions [50]. Disruptions in energy systems, in general, can have immediate impacts for core business functions such as heating, cooling, equipment charging, data backup and transmission, and security monitoring and intrusion detection.

3.1.5 Decision Support and Quality Monitoring Systems

A key feature of data acquisition and advanced food processing applications is the capacity to use real-time data to enable real-time decisions [52]. To do this, data from multiple devices (e.g., sensors, computer vision systems, industrial control systems) are aggregated and analyzed, either on-site or through off-site cloud platforms of service providers [52]. For example, combinations of sensors, data mining, and analyses can be used as part of warning systems for the early detection of food safety risks in food processing facilities [53]. In other applications, fruit freshness monitoring and assessment systems can make use of internet of things (IoT) technologies, such as RFID sensor tags and wireless sensor networks, in smart packaging processes [54] and to ensure traceability and minimize spoilage at various points along the FVC [34]. Blockchain technologies are also contributors to systems focusing on cyberbiosafety and cyberbiosecurity [55]. In Canadian agriculture, the leading digital decision support platforms for farm management and precision agronomy, such as Bayer's FieldView and other agricultural technology providers, are operated by a small number of large multinational agribusiness firms [56]. These

and other similar platforms provide farmers with advanced technologies and data-informed insights to optimize agricultural practices, improve crop yields, and make informed decisions [56], [57].

3.1.6 Supply Chain Management and Optimization Systems

Real-time data processing and analyses are fundamental components of supply chain integration and management, enabling efficiencies and accountability to consumer expectations and trade requirements in a globalized food system [58]. Logistics, purchasing, and trading have benefitted significantly from IoT-enabled technologies, particularly in the areas of transportation, distribution, and inventory management [5]. The confidentiality, integrity, and availability of data streams and systems are essential to these functions. While safeguarding technologies such as blockchain may help to improve the security position of these processes, they are not yet risk-free [59]. The regulatory environment presents a challenge for blockchain technology adoption because the built-in anonymity of decentralized blockchain systems contrasts with government interest to ensure the safety and integrity of items serving the public good (e.g., FVC transparency, supply chain continuity, food safety). Addressing regulatory challenges and uncertainties and promoting a better understanding of blockchain technology are essential for its broader adoption [60]. Despite these limitations, blockchain-based platforms may offer several benefits for the agri-food system, including more secure record-keeping [61] and enhanced transparency and traceability across the supply chain. The ability of these platforms to track produce from farm to store enables quick identification of contamination sources, improving food safety and facilitating faster recalls [31]. Such platforms also contribute to sustainability by reducing waste through more efficient inventory management [31]. In addition to the digital infrastructure of IoT-enabled agri-food supply chains, their physical and geographic arrangements (e.g., size, location, number) reflect the desire for efficient, just-in-time production and delivery. For example, Canada's beef supply chain concentrates key processes within a small number of slaughter and meat processing locations [5] that constitute a "pinch-point" in the middle of the value chain. This is bracketed on one end by numerous smaller scale cow–calf operations, or cattle feeding operations, and on the other end by distributors and retailers. Dependence on technology increases as animals move through the production system. Any disruptions at supply chain pinch-points can have significant ripple effects throughout the entire chain and a significant impact on animal welfare.

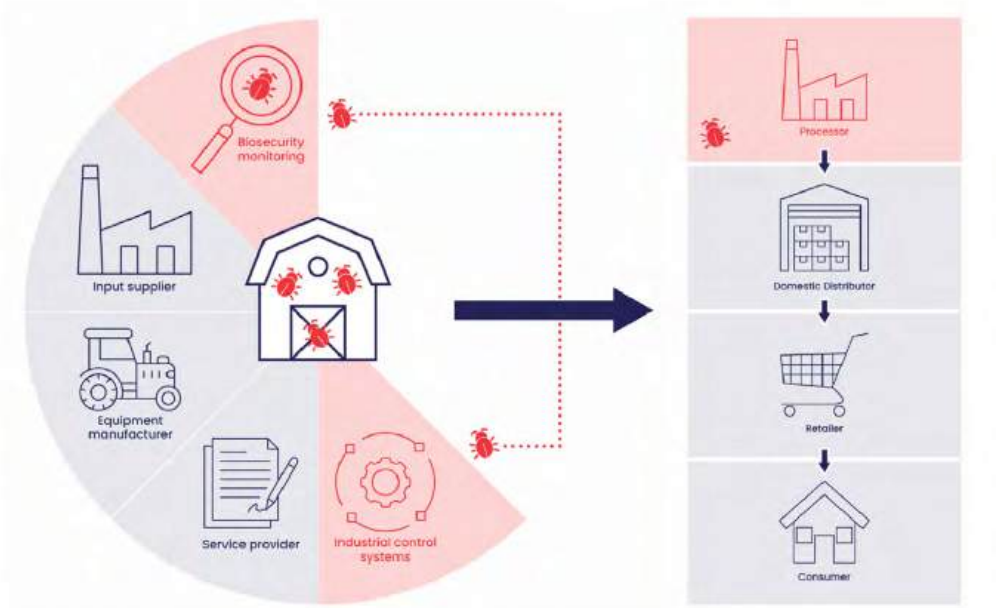
3.2 Recent Events, Future Hazards, and Emerging Opportunities

As the digital footprint of Canada's food system grows, so does the cyber threat landscape. This is illustrated by the number and type of malicious cyber incidents that have targeted the food CI since 2020. The focus of attacks has ranged from large processors such as JBS Foods and Maple Leaf Foods [62], to commodity sector entities such as Crystal Valley (grain) [63], L'Union des producteurs agricoles [64] and Lactanet [65] (dairy), as well as retailers such as Empire Company Limited (Sobeys) [66], and individual farming operations [67]. Table 1 provides a summary of these and other cyberattack examples. These types of incidents have overwhelmingly leveraged ransomware technologies to "lock up" data or systems in an attempt to extort money from agri-food sector parties. The Communications Security Establishment has identified ransomware as a top threat, in part because it falls under the "cybercrime-as-a-service" business model, which has been identified as a major threat to Canada [79]. Because of the transnational nature of certain cyber-criminal organizations, including hosting within the borders of adversarial countries (e.g., REvil in Russia [80]), there may be a geopolitical dimension to some of these events. In at least one reported case, a ransomware attack was perpetrated against a livestock operation by an activist group seeking to promote their ideological position [81]. The interconnected structure of the modern FVC, enabling just-in-time production and delivery, has limited slack, which offers a range of potential choke points to target. As shown in Figure 2, these multiple points of failure have been the focus of probing activities by malicious cyber actors.

Table 1: Examples of cyberattacks against the FVC since 2020 (from least to most recent, by category).

FVC Component	Date	Location and Details
Inputs/ Equipment/ Services	September 2021	**US:** $5.9M ransomware attack by BlackMatter against New Cooperative Inc., an agricultural services company for the grain, pork, and chicken industries [68]
	May 2022	**US:** Ransomware attack against AGCO, a manufacturer of precision agricultural equipment and infrastructure [69]
	August 2022	**US:** Demonstration of targeted compromise of a John Deere tractor's display/ control unit by white hat hacker and researcher, "Sick Codes" [70]
	April 2024	**Canada:** Attempted ransomware attack on dairy industry services company, Lactanet [65]
Primary Production	2022–2023	**Canada:** Dozens of ransomware attacks against individual farming operations in southern Ontario [71]
Processing/ Production	June 2021	**Australia, US:** Ransomware attack against JBS Foods, a giant multinational meat processor, temporarily shutting down facilities in North America and Australia [72]
	March 2024	**Belgium, US:** The Stormous ransomware gang attacked Duvel Moortgat Brewery, halting production at all Belgian and US sites. Attackers claimed to have stolen 88GB of data and demanded a ransom [73]
	June 2024	**Canada:** Customer data breach involving Quebec-based, farmer-owned, Agropur cooperative, one of the world's largest dairy processors [74]
Distribution/ Logistics	April 202	**Canada:** Unspecified cyberattack against parcel and courier business TFI International, a Quebec-based, North American transportation and logistics provider that also includes food transportation companies [75]
Retail/ Consumers	November 2022	**Canada:** Ransomware attack against Empire Company, Canadian owner of Sobeys grocery store chain with estimated $23M financial impact [66] and similar attack by Black Basta ransomware group targeting operations and confidential data (including customer data) at Maple Leaf Foods [76], [77]
	February 2023	**North America:** A ransomware attack against Dole Foods led to the shutdown of North American operations to contain its spread, halting grocery shipments, with some stores reporting outages of Dole products for several days [78]
	June 2024	**Canada:** A cybersecurity incident affecting Federated Co-op Ltd. disrupted internal and customer-facing systems, leading to Canadian inventory shortages of grocery items such as bread, frozen goods, fruit, dairy, and fresh produce [78]

Figure 2: Examples of elements within the FVC that may be targeted by cyberattacks (reproduced with permission [82]).



A diverse collection of digital technologies is in use across the FVC [52]. Cyber situational awareness and attention to cybersecurity as fundamental components of business risk management and development are underdeveloped within the agri-food sector, despite its CI status [83], reflecting the sector's varying levels of digital maturity. Because vast amounts of sensitive industrial data are exchanged, ensuring data protection is not just a regulatory compliance issue but is also a critical shield against industrial espionage and cyber threats [83]. Existing security solutions may focus on tactical system security, missing the strategic importance of considering how the privacy and protection of intellectual property may benefit from additional measures. The lack of transparency about how AI algorithms work (including issues of bias in the original coding or training data) is also a major issue [84]. Legislation touching on these algorithms and AI systems is pending [85] or a matter of public dialogue [86]. For example, Canada's proposed Artificial Intelligence and Data Act sought to create a common, and responsible, basis for the design, development, and deployment of AI systems [87]. In September 2023, Innovation, Science and Economic Development Canada released the Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems [88]. Signatories to the code committed to working to achieve a set of six outcomes, including accountability, safety, and transparency.

The agri-food sector is facing an increasingly complex threat landscape involving digital technologies and interconnected systems, which is characterized by the lack of a unified approach to security and the presence of various malicious actors. Together, these constitute a matrix of vulnerabilities and threats that loom over food system cybersecurity, domestic well-being, and national security. These challenges can be broadly categorized as those involving technology-based elements and those involving human-based social processes. Traditional technology-based cyber resilience frameworks for CIs often overlook the importance of relationships involving organizations and people within an ecosystem. These frameworks also tend to focus on business recovery rather than the opportunities to learn from and transform in response to evolving threat landscapes [11]. Research indicates that what helps organizations adapt to big challenges are people processes that connect organizations to

the resources they need when they need them [11]. In some cases, systems that face ongoing stressors can learn, adapt, and survive in the midst of evolving threat environments, becoming more resilient than those that remain isolated prior to encountering threats for the first time [11]. For example, during the COVID-19 pandemic, food system actors collaborated and modified their operations to sustain Canada's food supply chain despite the challenges imposed by the pandemic [89]. While the boundary between the technological and the human side of cybersecurity is soft, the distinction can point us toward critical gaps in understanding and preparedness, and a way of crafting a more comprehensive and responsive approach.

3.2.1 Technological Cybersecurity Vulnerabilities and Threats

Nikander *et al.* [90] used the Open Systems Interconnection (OSI) model to explore potential cybersecurity threats to the agricultural production component of the FVC. The OSI is a conceptual model that shows how different computer systems and networks communicate with one other. It breaks down the communication processes into seven role-specific layers. In cybersecurity, the OSI model helps professionals pinpoint where security measures may need to be applied. Each layer may have its own security protocols to protect data as it moves through the network. This model applies to computer system communications in general and is not specific to the FVC or the agri-food sector. It consists of seven layers that can be used to show how networks function, including identifying potential sources of problems [91]. Botschner *et al.* [5], [8] integrated previous applications of the OSI model [90], [92], [93] in relation to farm business functions, demonstrating the applicability of the OSI model to digitally enabled food production. An abbreviated description of these OSI layers, adapted from this work, is shown in Table 2.

A further iteration of the OSI model applicable to digital food system components was proposed by Botschner and Kotak [14] who added an eighth layer, dealing with the information space, to address the prominent role that human manipulation, or social engineering, often plays as an enabler of malicious cyber exploits. Importantly, this cognitive/semantic

Table 2: Overview of OSI Model layers relevant to digital agriculture architectures (adapted from [5], [8]).

	Terms Used for OSI Layers		Functions
7	**Edge and Cloud Layer**	Application Layer	Enables people to interact with computers and access network services.
6		Presentation/ Service Layer	Prepares data in a format that applications can use, which may include encrypting, processing, or analyzing the information.
5	**Network Layer**	Session Layer	Manages the ongoing connections that allow different software processes on an IoT platform (e.g., sensors, cloud services) to communicate with one another.
4		Transport Layer	Establishes the rules for how data are sent from one device to another to ensure reliable, end-to-end communication.
3		Network Layer	Determines how data travel across the network by directing traffic through switches and routers.
2		Data Link Layer	Specifies how and where data are organized and stored in a device's memory as they move through the network.
1	**Physical/Sensor Layer**		Handles the physical transmission of raw data between sensors, smart devices, and other hardware components.



layer is also the arena in which influence operations, such as misinformation or disinformation, and behavioural manipulations, such as phishing attacks, are conducted. Two review articles have highlighted critical vulnerabilities in agri-food systems and the cyber threats that exploit them. Kulkarni *et al.* [48] reviewed the key features of a set of cybersecurity incidents impacting the agri-food sector between 2011 and 2023, while Yazdinejad *et al.* [19] presented a new categorization of cybersecurity threats based on different stages of a cyberattack, organized in terms of the cyber kill chain (CKC) [94]. Kulkarni *et al.* [48] created a timeline of 397 cybersecurity incidents and 115 cybersecurity breaches [95] impacting the agri-food sector, based on the Verizon breach investigation report for the period 2015 to 2023 [96]. To inform mitigation strategies, based on a more comprehensive understanding of actual cybersecurity incidents in the food system, the researchers [48] selected a sample of 30 cybersecurity events for more detailed review. Although the majority of incidents (n = 22) occurred in the US, two occurred in Canada [48], and the remaining six affected agri-food sector organizations in Italy, the UK, Germany, and Israel. Most of the incidents (n = 17) involved ransomware attacks. This was followed by five data breaches, three malware-based attacks, two distributed denial of service attacks, and three incidents fitting other less defined categories. Thirteen instances of data losses were identified, along with 16 periods of service interruption, and 13 instances of financial losses, ranging from $2.5M to $202M (mean = $43.8M; median = $11M). No information was provided on the duration of service interruptions, the ongoing financial impacts on the affected organizations beyond the identified losses, or whether ransoms were paid to the attackers.

Yazdinejad *et al.* [19] identified IoT as one of the most consequential areas of risk, based on a review of digital agriculture technologies. Cybersecurity has been identified as an enabler of the safety and traceability properties of IoT connected food system supply chains [97]. New vulnerabilities introduced by IoT devices, such as those listed below, may open other critical systems to unauthorized control or breach in the FVC:

- Weak security settings: Many IoT devices come with default passwords or weak security settings that are easy for attackers to exploit. If these are not changed or strengthened, unauthorized users can easily gain access. The UK sought to address this vulnerability by passing the *Product Security and Telecommunications Infrastructure Act* 2022, which prohibits the use of common default credentials [98]

- Lack of encryption: If data transmitted by IoT devices is not encrypted, it can be intercepted by hackers. This can lead to unauthorized control of devices or the theft of sensitive information.
- Vulnerabilities in software: IoT devices often run on specialized software that may not be updated regularly. Outdated software can have security holes that hackers can exploit to gain control of the devices.
- Integration with critical systems: IoT devices are often connected to critical systems, such as irrigation, heating, or livestock management. If an IoT device is compromised, hackers could potentially gain access to these vital systems, disrupting operations or causing damage.
- Network exposure: IoT devices often connect to main networks. If these devices are compromised, hackers can use them as entry points to access other parts of the network, including sensitive data or farm-based command and control systems. Many businesses in the FVC are small and medium enterprises (SMEs), for whom network segregation is an important, but often misunderstood, security measure [99].
- Remote access: IoT devices are typically controlled remotely. If an attacker gains unauthorized access, they could manipulate devices remotely, leading to potential sabotage, theft of resources, or data breaches.
- Insufficient monitoring: Many SMEs may not have adequate monitoring or logging of IoT device activities. This can allow unauthorized access or breaches to go undetected for extended periods, increasing the risk of significant harm.

Newer approaches and threat actors that have yet to be reported in the literature are emerging, including ideologically motivated cashless ransomware attacks [81] and hybrid disinformation campaigns mounted against food system components to weaponize food security or international trade. Malicious cyber exploits are carried out in pursuit of a variety of objectives. For example, unauthorized entry into systems using stealth may take place to [19]:

- Explore and document features of systems;
- Steal data or intellectual property;
- Inflict damage to various components of a cyber-physical system; or
- Make unauthorized changes to systems and data (e.g., data poisoning, where data holdings or data in transit is manipulated to make it falsely appear that something is happening when it is not, or that something that is happening is *not* happening).

Each of these types of attacks can constitute an attack on data integrity, privacy, trust, confidentiality, and system availability. At a time when we are confronted by emerging public health challenges, data manipulation can pose a significant threat, as it may be used to cover up an emergent livestock disease, allowing it to develop to hard-to-manage proportions, or to make it appear that a problem like food contamination exists when it does not, creating alarm and undermining trust.

There is a distinction between confidentiality and privacy. Confidentiality involves protecting data from unauthorized access. Privacy is about giving individuals control over their personal data and ensuring it is handled according to their wishes. Both are crucial in cybersecurity, but confidentiality emphasizes security measures, while privacy is about data management and user rights. Growing attention on data ethics and ownership, and right-to-repair, suggest there is value to including confidentiality in cybersecurity initiatives focusing on the FVC [1], [100], [101], [102]. Yazdinejad *et al.* [19] identified six main groups of targeted components in digital agricultural systems, which can be mapped against the key security aspects of digital agriculture. This classification, with additional information, is summarized in detail in Table 3, and shows how readily generalizable Yazdinejad *et al.'s* analysis may be to FVC businesses more broadly, because all of the components and threat examples described in Table 3 can be found in a range of digitally enabled businesses across the FVC.

Table 3: Classification of targeted components in digital agricultural systems mapped to key security aspects (adapted from [19]).

Component/Definition		Illustrative Examples/Focus		Security Aspects
Attacks on Hardware	Targeting unknown or unsecured vulnerabilities by skilled attackers using advanced tools.	**Side channel**	Observing physical signals or conditions to illicitly infer information about how a system operates.	Confidentiality
		Radio frequency jamming	Disrupting the performance of a wireless network.	Availability
Attacks on Networks and Equipment	Focusing attacks on networks and connected systems or devices.	**Denial of service**	Employs multiple techniques to block or disrupt access to a communication channel or network element, such as an access point.	Confidentiality Privacy Availability
		Botnets	Collections of compromised devices or software agents ("bots") that are remotely controlled to carry out automated activities over the internet, such as spreading malware, stealing information, sending spam, or flooding websites with traffic to disrupt or disable them.	Integrity Availability Trust
		Man-in-the-middle	Stealth-based interception of communications between two or more parties. The interceptor can read, change, or block the transmission. Because the presence of the interceptor is unknown, it is a serious security risk.	Confidentiality Integrity
		Cloud computing	Making use of features of cloud platforms to propagate malicious exploits, at-scale, to other systems connected through a cloud environment.	Integrity Trust
Attacks on Data	Attacking data while it is being transmitted, stored, or actively processed within a system.	**Data leakage**	Illegal transmission of an organization's data by an internal source (either a person or device) to an external destination.	Confidentiality
		Cloud data leakage	Unauthorized exposure of data pertaining to an organization's users or its services, leading to a violation of user or party privacy.	Confidentiality
		False data injection	Supplying malicious information or control commands to a system.	Privacy
		Ransomware	Gaining illegal access to a system and encrypting critical digital assets, until a ransom is paid by the affected organization/ individual, at which time a decryption key will be provided.	Integrity
		Misconfiguration	Configuring reporting systems to reflect invalid information about the management of an operation, to misdirect business critical decisions.	Privacy Trust Integrity

Component/Definition		Illustrative Examples/Focus		Security Aspects
Attacks on Code	Identifying and exploiting flaws in software code to gain unauthorized access, extract data, or disrupt system functionality.	**Software update attacks**	Disrupting update processes of installed software.	Integrity Availability
		Malware injection	Installation of malicious code in various elements (e.g., devices) within a system.	Integrity
		Indirection (SQL injection)	Insertion of malicious code into a website's database through a form or input field (e.g., search box, login form), which can trick the website into revealing sensitive information, such as passwords, or enable an attacker to take control of the database.	Trust
		Buffer overflow	Software coding error or vulnerability that attackers can exploit to gain unauthorized entry to business systems.	Availability
Attacks on Hardware	Attacking the interconnected network of organizations and systems (vendors, consultants, and service providers) that collectively deliver security solutions and services.	**Third party**	Infiltrating a system through an outside partner or provider who has access to the system and/or its data.	Integrity Confidentiality
		Data fabrication	Creating malicious data or processes by misusing access provided for different purpose.	Integrity
Misuse Attacks	Abusing an organization's systems and operational structures as a platform to launch attacks against other targets.	**Cyber terrorism**	Using IoT systems and cyber-physical devices to attack businesses, systems, or people for violent ideological purposes.	Trust
		Invalidation and compliance	Using fabricated data to disrupt a valid certification of a process or transmission.	Integrity

Yazdinejad *et al.* [19] assessed the correspondence between this classification of attacks and the various stages of the cyber kill chain (CKC), a model of malicious cyber exploits that can be used to understand the sequential features of complex attacks. Figure 3 details the relationships among the seven stages of the cyber kill chain and the preparation, intrusion, and breach phases of a cyberattack. The first phase (preparation) involves collecting information on targets and their vulnerabilities, then developing an exploit package to take advantage of these vulnerabilities. The second phase (intrusion) involves deploying the exploit against the target to compromise their system(s) so that malware can be installed, data can be stolen, or other ways of access and removal can be put in place. The final phase (breach) involves consolidating control over the target network to fulfill the objectives of the cyberattack. Based on their review of available descriptions of cyber exploits, Yazdinajad *et al.* [19] found that leading-edge agri-food system cyberattacks commonly focus on several OSI layers to gather information during the reconnaissance stage of the cyber kill chain and to initiate attacks at subsequent stages. Depending on attack objectives, an attack method may be used against more than one layer—potentially within the same exploit—and may also serve the needs of more than one cyber kill chain stage.

Yazdinejad *et al.'s* [19] cyberattack framework is combined with Botschner and Kotak's [14] modified OSI model in Figure 4 to offer an integrated perspective on the relationship between the threat environment and digital agricultural systems. Because cybersecurity within the FVC has typically focused on agricultural production, the crosswalk of threats and vulnerabilities shown in Figure 4 centres on agriculture. For example, it shows how sensors and smart devices are key entry points for an attack in the physical sensor/control layer can be, and phishing emails or influence operations are used to manipulate human behaviour as part of the initial phase of a cyberattack in the human thinking/meaning layer.

According to the research conducted for this report, no such in-depth analysis has been carried out on other elements of the FVC, or on the value chain as a whole. However, because food processing, manufacturing, transportation, processing, distribution, and retail share many of the general categories of devices and IoT-enabled functions, a similarly complex and multi-faceted threat environment can be inferred for these components of the FVC as well. For example, the use of sensors and robotics in advanced processing or logistics could be susceptible to threats from similar points along the cyber kill chain. Furthermore, the daily volume of social engineering exploits, including emails,

Figure 3: Cyberattack stages based on components of the cyber kill chain (adapted from [19], [94], [103]).

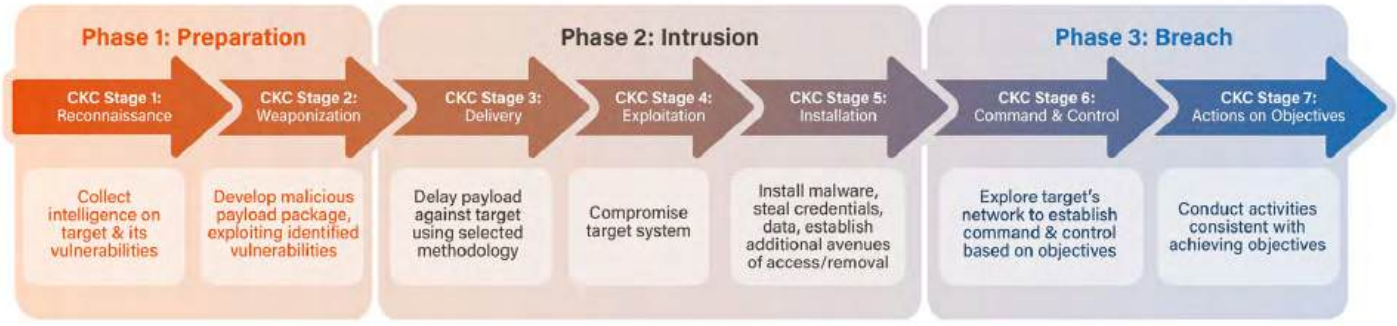
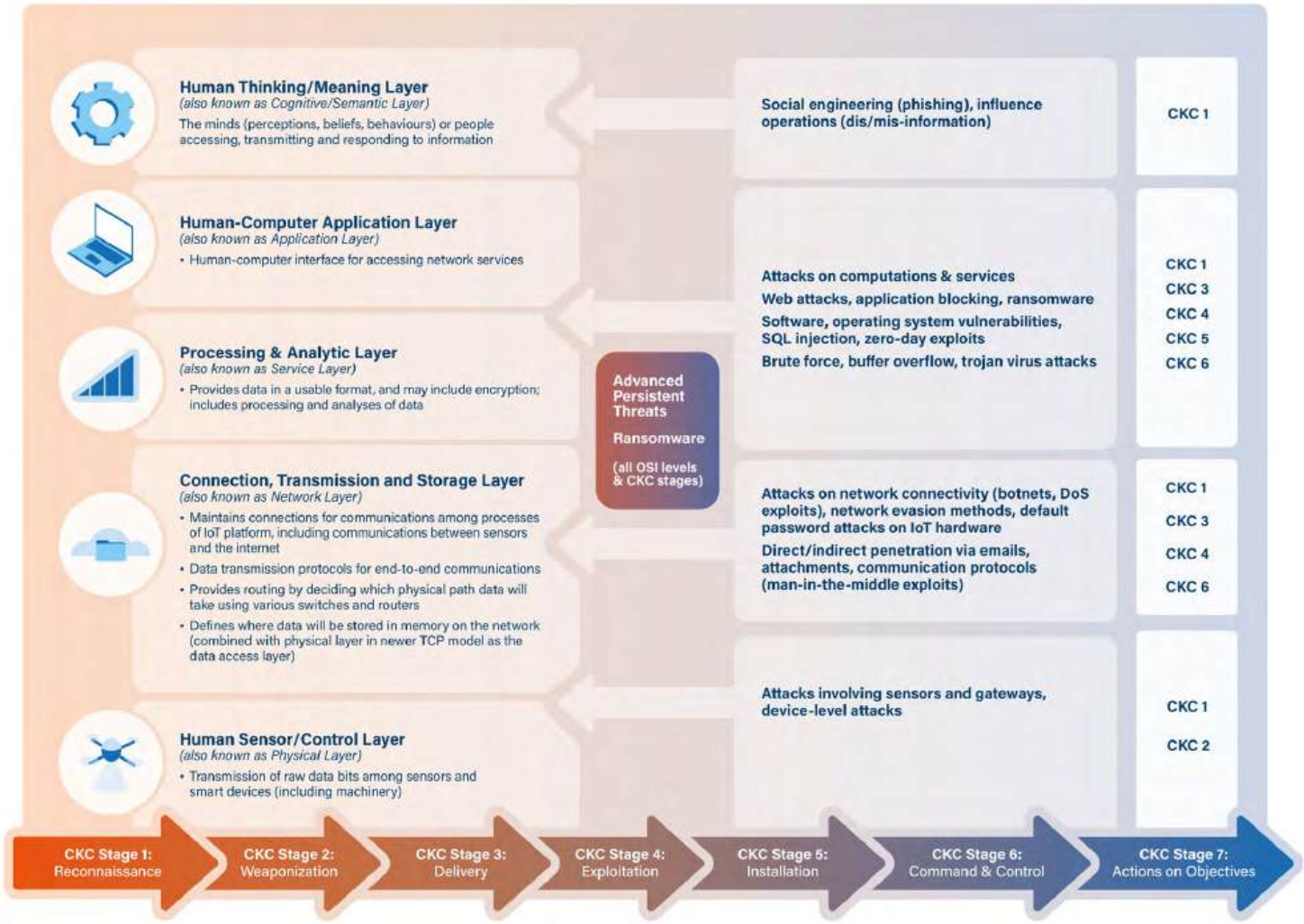


Figure 4: Common digital agriculture cyber threats and typical uses within the cyber kill chain (adapted from [19] and mapped to modified OSI model for digital agriculture [14], reproduced with permission from the Community Safety Knowledge Alliance).



text messages and, increasingly, deepfaked audio and video, suggests that the human thinking/meaning layer is becoming a greater focus for malicious cyber exploits. Based on their analysis, Yazdinejad *et al.* [19] proposed the following set of ten technical countermeasures against cyberattacks targeting digital agriculture that cover the most common layers/threats and encompass all five security aspects:

- User authentication;
- Secure passwords;
- Device-level encryption;
- Communication-level encryption;
- Port hardening (i.e., securing ports, or entry points, on a computer or network to prevent unauthorized access by closing unnecessary ports, applying strong security settings to those that remain open and monitoring them for suspicious activity);
- Remote login deactivation;
- Regular firmware updates;
- Safe password recovery;
- Unauthorized account deactivation; and
- Periodic device evaluation.

Although these countermeasures are evidence-informed, they warrant ongoing evaluation to ensure that they continue to play a constructive role in mitigating cyber threats. In considering a roadmap for further action, Yazdinejad *et al.* [19] highlighted several areas for attention, including avenues for further research. These areas reflect three overlapping levels of action: (a) research and practice development; (b) awareness and knowledge acquisition; and (c) policy and legislation. While all of these address the cybersecurity needs of the broader agri-food ecosystem, it should be noted that the best available research to date focuses largely on the agricultural production component of the FVC. The areas for consideration are summarized by level of action in the following paragraphs.

Research and Practice Development

- Access control. Unauthorized access (both physical and electronic) is a stepping stone to some of the most serious attacks on food system infrastructure. Three essential access control areas to consider are: authentication, authorization, and accounting.
- Data protection. This overlaps with cybersecurity (and information security management). However, data protection is a critical area of concern that should be the subject of focused attention from the perspective of research, education, practice, and policy.
- Network infrastructure and physical layer protection. These layers, which are foundational to digital food systems, are a common focus of attacks. Similar to data protection, they warrant more attention in research and practice development.
- Secure communication protocols specific to digital agriculture. Communication protocols are critical for operations that use remote sensors, autonomous equipment, and industrial control systems. While a variety of protocols for network, machine-to-machine (M2M), and IoT communications have been adopted from other domains, secure protocols specifically developed, tested, and standardized for digital food systems may be beneficial.
- Secure smart devices. Security-by-design should be a standard element in the development, testing, and manufacture of smart devices used within the FVC.

Awareness and Knowledge Acquisition

- Education as risk reduction. This addresses a social dimension of cybersecurity risk often absent in the literature, but which has begun to receive attention in the Canadian context [104].

Policy and Legislation

- Secure AI adoption. New and various applications of AI, including machine learning and natural language-based platforms such as generative AI, are becoming increasingly available to equipment manufacturers and service providers (including cybersecurity providers). These same technologies are already being leveraged by malicious cyber actors to enhance the scale and success of their exploits (e.g., the use of synthetic media or "deepfakes" to add realism to voice or image-based social engineering exploits).
- Legal frameworks. Policymakers can create useful legal and regulatory tools that safeguard private data and ensure the privacy of personal information. For example, Australia's Cyber Security Act 2024 requires organizations to report if they paid ransoms or face fines [105], although small business are exempt: "where entities with an annual turnover of less than $3 million are considered to be small businesses and exempt from reporting requirements of notifiable data breaches" [106].

3.2.2 Use Case Scenarios

The reviews by both Kulkarni *et al.* [48] and Yazdinejad *et al.* [19] described updated approaches for risk mitigation, greatly extending original research conducted by Nikander *et al.* [90] and others, and deepening results reported by Botschner *et al.* [5]. However, the persistent value of the following set of eight cyberattack scenarios identified in a 2018 report by the US Department of Homeland Security [107] should also be noted. These hypothetical scenarios covered threats to confidentiality, integrity, and availability:

Threats to Confidentiality:

- **Scenario 1:** Data exposure and theft (insider, outside malicious hacker) of farmer cooperative member data.
- **Scenario 2:** Foreign government gains access to confidential sensor data, which can be used to bias trade negotiations and/or to provide insights into features of CI.

Threats to Integrity:

- **Scenario 3:** Data poisoning (realistic fake data) and public exposure to mimic a crop or livestock disease outbreak, disrupting supply chain function and causing reputational harm and damage to public trust.
- **Scenario 4:** Alteration of data in transit to disrupt sensor or decision support systems, resulting in harm to or loss of crops or livestock.
- **Scenario 5:** Alteration of data or algorithms used in livestock breeding processes, leading to financial losses due to missed gestation windows.

Threats to Availability:

- **Scenario 6:** Compromised software (e.g., compromised patches, off-brand packages to "jailbreak" equipment as part of "right-to-repair" approach to equipment maintenance) with exploitable vulnerabilities or malicious backdoors, which could result in equipment malfunctions or intentional disruptions during critical planting or harvesting windows, ransomware attacks, and other malicious exploits perpetrated against the business or other connected data entities.
- **Scenario 7:** Equipment manufactured abroad incorporating firmware that enables various remote access functions. Remote access tools that have been installed by, or at the behest of, a foreign actor could enable destructive equipment attacks on the agri-food sector.
- **Scenario 8:** Where rural communications systems lack redundancy and resilience, natural disasters may disable the guidance or communication systems required for the operation of precision agriculture tools.

While these threat scenarios are all relevant to the Canadian agri-food system, in the present environment of climate emergencies, disease outbreaks, and global unrest, scenarios 2, 3, 5, and 8 are particularly relevant.

- **Scenario 2.** Access to unmanned aerial system sensor data by foreign entities could become a concern for Canada, especially if key agricultural data is transmitted to, or stored by, foreign entities that are seeking to weaponize food security. Foreign access to, and tampering with, sensor data could advantage an adversary for economic or strategic gain.
- **Scenario 3.** Data poisoning to simulate a livestock or crop disease outbreak could have severe consequences for Canadian agriculture, causing economic and reputational damage. This is especially relevant in large-scale farming and livestock production, where real-time monitoring is critical. Data poisoning exploits could be conducted to harm Canada's trading relationships or as a pretext by a hostile foreign government to weaponize trade as part of a hybrid operation within a diplomatic dispute. Additionally, this scenario aligns with use cases that depend on real-time IoT data for decision-making, as tampering with sensor data could lead to false alerts of disease outbreaks in crops or livestock.
- **Scenario 5.** With the application of AI to genomic analyses, stolen livestock breeding data could be examined for strain-specific resistance or vulnerabilities to disease or climate conditions in ways that could be commercialized by corporate or foreign competitors, or weaponized by the latter.
- **Scenario 8.** Climate-related and other natural disasters could disrupt rural communication networks and render digital agriculture systems inoperable. This threat is potentially intensified by the vast distances separating some of Canada's rural farming communities from timely access to support for repair and recovery. Moreover, this scenario highlights the need to develop resilience in rural communication systems as a protective measure for Canada's vast rural farming operations.



"Three leading cognitive biases related to socially derived cybersecurity risks are particularly relevant: (a) misplaced optimism, (b) inertia or loss aversion, and (c) present bias."

3.2.3 Social Cybersecurity Vulnerabilities and Threats

The preceding discussion regarding FVC cybersecurity focused on technical systems and vulnerabilities. However, the root of all cybersecurity challenges lies in the human dimension. Social cyber vulnerabilities and threats are a composite of human intentions and human error [108], along with group, business, and system-wide practices [109], [110]. As the agri-food system is a CI and a contributor to national security, a range of strategic actions involving the human dimension may be necessary to predict, prevent, and detect malicious cyber exploits [5].

3.2.2.1 Individual Factors Limiting Cyber Preparedness

Several individual-level factors have been identified as possible barriers to improving the cyber preparedness of businesses within Canada's FVC, including awareness, uncertainty and lack of knowledge, stigma, and cost considerations. Each of these factors is also related to misperceptions and misunderstandings of risk that are common in everyday life. These result partly from the mental "shortcuts" (i.e., cognitive biases) that people use to manage the moment-to-moment flood of information that reaches our senses [5]. Dupont [111] and Dupont *et al.* [112] suggested several ways that people's thinking habits can bias perception of cybersecurity risks, which may result in a misplaced sense of safety among business owners. Three leading cognitive biases related to socially derived cybersecurity risks are particularly relevant: (a) misplaced optimism, (b) inertia or loss aversion, and (c) present bias.

Misplaced Optimism

Optimism bias is the tendency to believe that we are less likely to experience negative events compared to others [113]. This bias can lead to underestimating risks and making overly positive predictions about the future. It has been found that this bias negatively impacts cybersecurity in two ways: individuals misperceive risk and they see themselves as not being vulnerable to cyber threats [114]. In Canada, a survey found that the idea of "security through obscurity" and the attitude of "it won't happen to me" were present among agricultural sector business owners [6]. Anecdotal information gathered through conversations during that research suggested a potential relationship between the sense of invulnerability and the presence of stigma around being victimized. This emerged in conversations with producers and other business owners who acknowledged that no one wanted to be seen as an unwitting victim because that conflicted with the social desirability of being a savvy agricultural business owner. It is important for sector business owners to understand the potential consequences of not sharing experiences of victimization, which may create the impression that cyberattacks are less prevalent than they are, leading to a false sense of security among others within the sector. There is a need for systematically gathered occurrence data among those who monitor and respond to cybersecurity incidents within the FVC. It is also suspected that cyber incidents are significantly

underreported (e.g., [67]). Optimism bias may lead an individual to engage in a number of behaviours that make businesses more vulnerable to cyberattack, such as sharing credentials, sidelining preventive measures, ignoring indicators of potential security incidents, or being overconfident about their ability to manage cybersecurity [114]. These findings suggest the potential value of a two-pronged strategy: (a) raising awareness about cybersecurity in the FVC in general, and (b) showcasing specific examples of cyber incidents that have affected Canadian businesses. Dehghantanha and Karimpour [115] conducted a market survey of agri-food parties in Canada and the US to study cybersecurity technology adoption and perceived requirements, and found that concern about cybersecurity as a business issue was assessed at only a moderate level. More encouragingly, Russell *et al.* [116] found that, although there was variability in risk perception among the producers they interviewed, it appeared to be increasing over time. Specifically, participants reported that anecdotal information about cyberattacks happening around them, or learning about cyberattacks in the news, impacted their awareness. However, estimates of personal levels of risk did not seem to correlate with estimates of risks to their farm businesses, regardless of other variables, such as producer age, size of the farm, or the amount of digital agricultural technology being used.

Inertia Bias or Loss Aversion

Inertia bias is the tendency to choose to remain with the current situation, even when there may be better alternatives available [117]. This is also known as loss aversion, which emphasizes that negative changes from a reference state (losses) tend to be more salient to people than positive changes (gains). This bias can lead to resistance to change or to making decisions that prioritize maintaining things as they are, rather than adopting new and potentially more beneficial choices. Inertia bias and loss aversion may provide an additional explanation of some study findings. For example, in the survey of producers discussed in [6], 52 percent of respondents indicated that on-farm cybersecurity was not a farm business priority. This was reinforced by farmers reporting an average spend of just over $500 on cybersecurity between January 2020 and January 2022. In comparison, a Canadian Federation of Independent Business survey found that small businesses spent an average of $6700 on securing information technology (IT) systems during the same period [118]. Similarly, Dehghantanha and Karimpour's analysis of market trends in digital agriculture found that cybersecurity spending in this sector accounted for only two to three percent of the total cybersecurity market in North America, despite the rapid growth of the latter market and the steady growth of digital technologies across the food system. As of 2019, the compound annual growth rate of the digital agriculture technology market and the global cybersecurity market were 14.1% and 10%, respectively [115]. Although there is currently no established corporate spending benchmark for cybersecurity, as a percentage of global revenue [119], some sources recommend a range of 5% to 20% of a business's IT budget [120]. For smaller businesses, where the IT budget is a small share of business revenue (less than 5%), spending on cybersecurity may easily account for less than 1% of total revenue [121]. Statistics Canada reports that, in 2023, the agri-food sector accounted for approximately 7% of the country's GDP [122]. Farm business cycles typically correspond to growing seasons, rather than business quarters used in most other non-farm businesses. What may appear to be slower decision-making may actually be a function of the unique pace of farm businesses.

Present Bias

Also known as myopia bias or short-termism, present bias is the tendency to focus on present benefits rather than future harms. While farmers generally do well to anticipate future states (e.g., commodity prices), they and other small- and medium-sized FVC businesses adopting digital technology may not integrate the full range of short- and long-term issues into their analysis [123]. Present bias is particularly challenging for cybersecurity risks, which are often poorly understood by smaller businesses, as noted when considering optimism bias and inertia bias. Consequently, producers and others are likely to overemphasize current challenges at the expense of uncertain future cyber risks associated with new digital technology. Interviews conducted with agri-

commodity organizations between 2021 and 2022 [6] found that, while organizations were taking steps to secure their own digital assets, few were focused on mobilizing awareness and building knowledge among the producers they served. In 2021, a meeting of the Federal-Provincial-Territorial Ministers of Agriculture led to the Guelph Statement [124], which articulates a set of shared priorities and principles guiding the development of the agri-food sector policy framework from 2023 to 2028. Although the Guelph Statement prioritizes "science, research and innovation to address key challenges and opportunities" and "enhancing resiliency to anticipate, mitigate and respond to risks," as well as emphasizing the principle of collaboration with all key actors, it does not explicitly identify the role of digital agricultural technologies, nor the role of cybersecurity as an enabler of these technologies.

3.3 Enhancing Preparedness and Resilience

Improving cybersecurity preparedness and resilience across the FVC requires a combination of individual practice changes, system-level efforts, and processes that bridge individuals and systems to create networked capacity. The "cyber barn raising" framework was developed as part of the CSKA's cybersecurity in agriculture research project, which focused on protecting primary agricultural production [11]. The framework, which is shown in Figure 5, outlines the key conditions needed to strengthen cyber resilience in agriculture and specifies four pillars of action to enhance cybersecurity preparedness and resilience in this part of the FVC.

On-Farm Cybersecurity

With the increasing presence of networked digital technologies within the agri-food system, cyber threats are becoming more widespread and more complex. Those managing enterprise-level risks and those at the front lines of food safety and security bear the brunt of cybersecurity pressures. While adopting cybersecurity best practices is critical, producers, processors, distributors, and retailers should not be left to manage these risks alone. The cyber barn raising framework proposes that cybersecurity capacity building should begin with these groups in mind, but should also build security and resilience by involving all key actors.

Cross-Sector Partnerships

Managing relevant business risks and opportunities should be a shared concern. This is consistent with the perspective that a key property of value chains is a shared commitment to understanding and addressing collective risk [23]. To build a resilient

Figure 5: The cyber barn raising framework for cyber resilience within the agricultural sector (adapted from [11]).



and adaptive food system, collaboration is essential. In Canada, due to a lack of domestic collaborative platforms, most CIs rely on US initiatives (e.g., the Food and Agriculture Information Sharing and Analysis Center [125]). To strengthen planning and response capacity, greater collaboration across sectors will be required to predict, deter, and prevent cyber incidents. This approach advocates for the inclusion of diverse perspectives, ensuring that a wide range of interested parties, such as farmers, industry groups, NGOs, academics, government, other CI operators and consumers, are involved.

Workforce Capacity

A workforce that includes knowledge, skills and abilities related to cybersecurity is crucial for innovation and economic growth. To that end, the cyber barn raising framework specifies two key activities: (a) providing ongoing training for people already working in the agri-food sector and (b) preparing youth and new entrants through post-secondary education. The global talent shortage in cybersecurity is estimated to be in the millions [126]. Beyond traditional STEM training, post-secondary programs should incorporate cybersecurity awareness across other fields, including agriculture, business, and technology. Early education for children and youth is also important to inspire future careers in the agri-food sector. By focusing on both current and future talent, Canada can address the growing cybersecurity challenges across industries.

Legislation, Governance, Standards and Incentives

Effective data governance is indispensable for managing the complex processes, opportunities, and risks associated with digital agriculture technologies. It enables trust in the people, processes, and technologies, which is foundational for innovation and adoption. Governance structures for cyber resilience should be tailored to meet specific needs, recognizing that digital agri-food technology is an interconnected and interdependent ecosystem. Standardization could play a key role in advancing cyber governance, maturity and resilience in Canada's agri-food sector by helping to safeguard data availability, integrity, confidentiality, and ownership. For example, a 2023 report from the International Organization for Standardization (ISO) Strategic Advisory Group on Smart Farming highlights practical opportunities for enhancing digital agricultural cybersecurity through standardization [127].

3.4 Jurisdictional Cybersecurity Frameworks and Guidelines

3.4.1 Canada

In 2019, a mid-term review of the 2019–2024 National Cyber Security Action Plan [128] and the National Cyber Security Strategy was launched by Public Safety Canada [129]. Although the FVC was not identified explicitly as a focus for action on CI cybersecurity, the 2021 cyberattack on JBS Foods was highlighted to draw attention to the real-world consequences of malicious cyber activities. Agriculture and Agri-Food Canada created a web page, Cyber Security and Your Farming Business [130], to disseminate resources on cybersecurity to producers. In addition to practical advice on potential business practice changes, the page includes links to a variety of resources [131], [132], [133]. In 2024, Agriculture and Agri-Food Canada established the Working Group on Cyber Security in the Agriculture and Agrifood sector, which includes representatives from the federal, provincial, and territorial governments, along with representatives from the agri-food industry and research communities, and focuses on:

- Facilitating discussions and collaboration among senior officials and cybersecurity experts on emerging threats and trends affecting agriculture and agri-food sectors;
- Identifying gaps and opportunities (e.g., standards, policies, best practices) to improve cybersecurity resilience in the sector; and
- Supporting the development and dissemination of resources to raise awareness of cybersecurity threats and guide the agricultural sector, especially SMEs, in building cybersecurity resilience.

In 2024, Ontario launched the Cybersecurity Preparedness Initiative to provide financial support to cybersecurity enhancements addressing the "specific and growing needs of agricultural marketing boards" [134]. This program provides funding

for cybersecurity improvements. At the time of writing, no other province or territory has launched cybersecurity funding programs for the agri-food sector, although British Columbia has launched its CyberBC initiative, which focuses on broader public sector organizations [135]. The Canada Cyber Foundry at the University of Guelph was created with support from the governments of Canada and Ontario and includes a non-profit consultancy, as well as education, training, and self-assessment tools that focus on the needs of SMEs [136] within the FVC.

In Canada, the most formal organizing frameworks for cybersecurity that could be applied to the FVC are the Canadian Centre for Cyber Security (CCCS) Baseline Cyber Security Controls for Small and Medium Organizations [137], new federal legislation (Bill C-26) that would enact the Critical Cyber Systems Protection Act [138], and a set of voluntary Cyber Security Readiness Goals (CRGs) for federally regulated CI operators (banks, telecommunications, transportation) [139]. Any organization doing business with regulated entities will likely be contractually obligated to meet the same requirements (e.g., reporting, audited cyber plan, etc.). CCCS assessed that while it would be optimal for businesses to implement a set of Canada-specific cybersecurity controls (a policy, tool, or procedure that reduces the risk of a cybersecurity incident affecting digital systems, networks, and data) comparable to the National Institute of Standards and Technology (NIST) Cyber Security Framework or ISO/IEC 27001 (Annex 4A) [140], that may be out-of-reach for many SMEs due to financial and human resource constraints. Consequently, CCCS formulated its baseline cyber security controls to be useful to small and medium-sized organizations in Canada, and two further assumptions were made in developing the controls:

- Organizations can address most cyber threats through cybersecurity awareness and best practices in cybersecurity and business continuity; and
- The 80/20 rule is relevant in achieving tangible advances in cybersecurity, where 80% of the benefits can be achieved with an initial 20% of the effort.

As shown in Table 4, CCCS identified five organizational controls (i.e., actions to help organizations determine whether the baseline controls are relevant for their specific circumstances) and 13 baseline controls "to help organizations maximize their cybersecurity investments" [137].

Bill C-26 [141], which advanced to second reading in the Senate in June 2024, offered a framework for safeguarding cyber systems crucial to Canada's national security and public safety. The bill mandated that designated organizations ("vital services" or "vital systems") must:

- Develop and implement cybersecurity programs;
- Mitigate supply chain and third-party risks;
- Report supply chain and third-party risks; and
- Adhere to cybersecurity directives.

While these provisions do not refer directly to agri-food sector organizations, they are a set of conditions and obligations that are relevant across the agri-FVC. Bill C-26 died on the order paper when Parliament was prorogued in January 2025, but in June 2025, similar legislation was introduced under Bill C-8 [142], which advanced to second reading in the House of Commons in October 2025 [143]. The *Consumer Privacy Protection Act* contained within Canada's *Digital Charter Implementation Act 2022* (Bill C-27), focused on strengthening private sector privacy law [121]. Among other things, the Act addressed reporting to the Office of the Privacy Commissioner of Canada if the risk of significant harm threshold is met. Failure to do so would result in significant administrative monetary penalties. This would formalize a stronger reactive stance but it does not directly address proactive approaches to prevent data breaches in the first place. Bill C-27 also died on the order paper in January 2025. In October 2024, CCCS published the CRGs, a set of guidelines for CI operators to assist in enhancing the cybersecurity posture of essential services. Notably, the CRGs, which are "designed to be an evergreen resource that can be used by all critical infrastructure sectors. . . will be updated by the Cyber Centre based on feedback from partners and as the threat landscape evolves over time" [144]. Included in this resource is a toolkit of 36 cross-sector cybersecurity practices that have been designed to be applicable to all CI.

Table 4: Canadian Centre for Cyber Security organizational controls and baseline cybersecurity controls (adapted from [137]).

Organizational Controls	Baseline Cybersecurity Controls
1. Assess organizational size ▪ The baseline controls were intended to serve organizations with less than 500 employees. ▪ It is recommended that larger organizations invest in more comprehensive cybersecurity measures.	1. Develop an incident response plan 2. Automatically patch information systems and operations 3. Enable security software 4. Securely configure devices 5. Use strong user authentication 6. Provide employees with awareness training 7. Back up and encrypt data 8. Secure mobility 9. Establish basic perimeter defences 10. Secure cloud and outsourced IT services 11. Secure websites 12. Implement access control and authorization 13. Secure portable media
2. Determine what IT is in scope ▪ Organizations should identify which components of their information systems and assets fall within the scope of their implementation of the baseline controls. They should also provide a justification for excluding any information systems or assets and acknowledge the associated risk in doing so.	
3. Determine the value of information systems and assets ▪ Organizations should ensure they comprehend the value of their information systems and assets (e.g., sensitive customer information and intellectual property). ▪ Organizations should evaluate potential harms on the confidentiality, integrity, and availability of their information systems and assets.	
4. Confirm the cybersecurity threat level ▪ Organizations should identify whether experiencing a cybersecurity incident would not just cause harm against the organization but might also constitute a threat to national security.	
5. Confirm cybersecurity investment levels ▪ Organizations should identify personnel accountable for a leadership role in ensuring cybersecurity. ▪ Organizations should determine acceptable resourcing levels (financial and human) related to cybersecurity. ▪ Organizations should commit to ongoing improvements in cybersecurity.	

Like the Baseline Cyber Security Controls for Small and Medium Organizations [137], the voluntary CRGs represent an attempt to create a practical pathway to a better cybersecurity posture, rather than enshrining a comprehensive and exhaustive list of requirements. A helpful dimension of the CRGs for the agri-food sector is that they include cybersecurity recommendations that cover both IT, which focuses on managing and processing information, and operational technology (OT), which involves controlling and monitoring physical processes and systems. As shown in Table 5, the CRGs are organized according to six pillars that reflect and add to the organizing framework used in the US Government's NIST Cybersecurity Policy Template [145], and which extend the US Cybersecurity and Infrastructure Security Agency's (CISA) Cross-Sector Cybersecurity Performance Goals [146]. Each of the 36 CRGs provided in the Cross-Sector Cyber Security Readiness Goals Toolkit [147] is elaborated on and linked to references that provide additional information on implementation. Five aspects of effective implementation are specified, and are outlined in Table 6. These five elements are intended to serve a variety of CI situations and to complement the Baseline Cyber Security Controls for Small and Medium Businesses [137]. However, unique features of enterprises within the FVC may preclude the implementation of some of these safeguards. This will be discussed in further detail in Section 3.7, which summarizes findings from the interviews.

Table 5: Canadian Centre for Cyber Security CRGs (adapted from [139]).

Pillar (*New)	Corresponding CRGs (*New, ** Altered)
Govern*	▪ Privacy leadership* ▪ Supply chain incident reporting process and policies** ▪ Vendor/supplier cybersecurity requirements ▪ Organizational and OT cybersecurity leadership** ▪ Improving IT and OT cybersecurity relationships**
Identify	▪ Asset inventory and network topology** ▪ Mitigating known vulnerabilities ▪ Third-party validation of cybersecurity control effectiveness ▪ Incident response plans ▪ Deploy security.txt files (a standardized way for organizations to provide information on how to report security vulnerabilities or security-related issues) ▪ Select a trusted cloud service provider*
Protect	▪ Change default passwords ▪ Minimum password strength ▪ Unique credentials ▪ Revoke credentials for departing employees ▪ Separating user and privileged accounts ▪ Network segmentation ▪ Detection of unsuccessful login attempts ▪ Phishing-resistant multi-factor authentication ▪ Basic and OT cybersecurity training ** ▪ Strong and agile encryption (data in transit) ▪ Secure sensitive data (data at rest) ▪ Email security ▪ Disable macros by default ▪ Hardware and software approval process ▪ System backups and redundancy ▪ Log collection ▪ Secure and central log storage** ▪ Prohibit connection of unauthorized devices ▪ Limit OT connections to public internet ▪ Document device configurations ▪ No exploitable services on internet ▪ Secure administrator workstation*
Detect	▪ Detect relevant threat and tactics, techniques, and procedures (TTPs)
Respond	▪ Incident reporting
Recover	▪ Incident planning and preparedness

Table 6: Implementation considerations for CRGs in cross-sector goals toolkit (adapted from [147]).

Aspect	Detail
Outcome	The intended security outcome intended for each CRG.
Recommended action	Actions to take to achieve CRGs (updated as required).
TTPs/risk addressed	Risk statement: The risk(s) mitigated by implementing recommended action(s). This includes, where applicable, reference to the MITRE ATT&CK globally accessible repository of adversary tactics and techniques derived from real-world observations. The ATT&CK knowledge base serves as a foundation for creating specific threat models and methodologies in the private sector, government, and cybersecurity products and services (https://attack.mitre.org/).
NIST CSF 2.0 reference	Subcategory of NIST 2.0 that best relates to the security practice of each goal.
Supporting guidance reference	Additional information and resources provided by the Cyber Centre in support of each goal and outcome.

3.4.2 United States

In March 2016, the Federal Bureau of Investigation (FBI) published a Private Industry Notification that identified smart farming technologies as a potential threat pathway for attacks against the US food and agriculture sector [148]. At that time, the assessed threat focused mainly on the potential theft of farm-level data. In addition to farm-level precautions, producers were encouraged to ask agricultural technology and other data management companies how they use and safeguard farm data, and what they do to integrate cybersecurity measures into digital agriculture technology. In 2018, the Department of Homeland Security's Public–Private Analytic Exchange Program issued a report on potential vulnerabilities related to digital agriculture, illustrating these through eight threat scenarios, as discussed in Section 3.2.2. The threat overview was based on the three pillars of information security: confidentiality, integrity, and availability. The report concluded with a set of recommended best practices for the producer and agribusiness communities. Eleven baseline security controls were proposed under three categories [107]:

- Key security controls used in other industries with applicability and utility in securing digital agriculture technologies and their users. These controls are derived from the Center for Internet Security (CIS) Critical Security Controls [149] and guidance from industry practitioners, and are:
  - Implement email and browser protections;
  - Limit and control network ports, protocols, and services;
  - Inventory and control hardware assets;
  - Inventory and control software assets;
  - Account monitoring and control; and
  - Separate operational technologies and business operations.
- Additional controls for operators of digital agriculture, to address issues not included in the key security controls:
  - Data recovery capabilities;
  - Data protection; and
  - Understanding data ownership.
- From a broader deterrence perspective, incident response and physical security for digital agriculture businesses:
  - Incident response and management; and
  - Implement physical controls.

A subsequent FBI Private Industry Notification in September 2021 flagged the growing threat of ransomware attacks on the agriculture sector and provided a set of recommendations focusing on basic cyber hygiene practices. At the time of writing, the CISA continues to recommend the 2018 Department of Homeland Security report for information and as a basis for threat mitigation [107], [150]. A 2018 report by the US Government Accountability Office on cybersecurity framework adoption across CIs recommended that the US Department of Agriculture (USDA) should consult with sector partners and relevant parties, including the Department of Homeland Security and NIST, to "develop methods for determining the level and type of framework adoption by entities across their respective sector" [151, p. 22]. Despite efforts to engage the agri-food sector, and to encourage and support the use of the NIST cybersecurity framework, as of February 2018, "the USDA has not yet received information from sector entities regarding their adoption of. . . the framework" but indicated a commitment to "providing its members with guidance on framework adoption in [that year]" [151]. In May 2021, the President of the US issued an Executive Order on Improving the Nation's Cybersecurity [152], which emphasized the importance of:

- Removing barriers to threat information sharing between government and the private sector;
- Establishing a cyber safety review board with the authority to convene following a significant cyber incident to analyze what happened and make concrete recommendations for improving cybersecurity; and
- Creating a standardized approach ("playbook") for responding to cybersecurity vulnerabilities and incidents.

In 2013, the IT Information Sharing and Analysis Center (ISAC) created the Food and Agriculture Special Interest Group to help the industry safeguard



agri-food enterprises. As demand grew, the group evolved to become the Food and Agriculture ISAC [125], which has three key functions:

- Document the tactics, techniques, and procedures of malicious cyber actors, as well as indicators of compromised technology or systems;
- Provide incident-specific alerts and publish requests for assistance on behalf of members; and
- Provide access to an intelligence management platform that members can use to enhance their capacity for threat hunting and analysis.

The relationship between CI operators and the US government is primarily regulatory rather than purposefully collaborative. US ISACs are relevant to Canadian cyber readiness because most domestic CI sectors collaborate with American ISACs, and Canada lacks a similar entity. The interconnected nature of North American CIs and Canada–US collaboration on defence and security may also be a factor. The Promoting Precision Agriculture Act of 2023 directed the USDA, in collaboration with NIST and the Federal Communications Commission, to develop voluntary interconnectivity standards and prioritize cybersecurity [153]. The Farm and Food Cybersecurity Act of 2025 [125], currently proceeding through committee approval, seeks to strengthen cybersecurity across the agri-food sector by outlining key measures for risk assessment and improving readiness to respond to cyber threats. CISA also conducts large-scale, biennial government-sponsored cybersecurity exercises, known as Cyber Storm, which featured the agri-food sector for the first time in April 2024 as the primary impacted sector in the simulation [154].

3.4.3 European Union

There are three central regulations in the EU that address cybersecurity: (a) the *European Union Agency for Cybersecurity* (ENISA) *Regulation,* (b) the Directive on Security of Network and Information Systems (NIS and NIS2 Directives), and (c) the EU General Data Protection Regulation (GDPR) [155]. Although the ENISA Regulation does not explicitly reference standards, the importance of pursuing enhanced cybersecurity through European standardization organizations and the ISO is identified [156]. The original NIS Directive [156], adopted in 2016, required EU member states to ensure that operators of essential services in sectors such as energy, transport, banking, financial market infrastructures, health, water supply, and digital infrastructure take appropriate security measures and report incidents. However, it did not explicitly mention the food sector. The directive required member states to ensure that essential services operators and digital service providers take appropriate security measures to manage risks to the security of network and information systems.

While the directive emphasized the importance of security measures, it did not prescribe specific cybersecurity standards. Instead, it allowed member states some flexibility in determining the standards and measures that should be implemented, which had to be proportionate to the risks. The NIS2 Directive [157], which updates and expands on the original NIS Directive, was implemented into law in the EU in 2024 [158], and broadens its scope to include more sectors and subsectors, including the agri-food sector. It also introduces stricter security requirements. Agri-food relevant provisions include:

- Essential entities: Food production, processing, and distribution are listed among the essential entities that must adhere to cybersecurity requirements.
- Increased scope: Medium and large enterprises in the agri-food sector are included in NIS2.
- Risk management: Entities in the agri-food sector must implement risk management measures, including those related to cybersecurity.
- Incident reporting: NIS2 mandates that significant incidents affecting the food sector be reported to national authorities.
- Corporate accountability: Management is directed to receive training on, and have oversight and approval of, measures aimed at addressing cybersecurity risks.
- Business continuity: Organizations are to take appropriate steps to enable business continuity in the event of cybersecurity events, including system recovery.

To date, seven member states have approved and adopted the implementing legislation: Belgium, Croatia, Hungary, Italy, Latvia, Lithuania, and Slovakia [159]. The percentage of the GDP of these countries accounted for by agriculture, forestry, and fishing ranged from 0.8% (Belgium, 2024) to 4.1% (Latvia, 2024), compared to 1.6% for Canada (2021) and 0.9% for the US (2024) [160]. The inclusion of the agri-food sector reflects the growing recognition of the importance of securing the sector, given its role in national and international supply chains. The NIS2 Directive expands and clarifies the requirements related to cybersecurity standards, as follows:

- Harmonized security measures: NIS2 introduces more specific requirements for risk management and mandates that essential and important entities implement technical and organizational measures to manage cybersecurity risks. These measures must be based on recognized international standards and best practices where applicable.
- European cybersecurity certification framework: This aims to create an effective level of cybersecurity standardization across the EU, and identifies that national frameworks should specify [161]:
  - Categories of products and services covered;
  - Cybersecurity requirements, such as standards or technical specifications;
  - Type of evaluation to be conducted; and
  - The envisioned level of assurance.
- Sector-specific standards: NIS2 acknowledges the need for sector-specific cybersecurity standards and encourages the adoption of these standards to ensure that security measures are tailored to the unique needs of different sectors, including the food sector.
- Guidelines and best practices: NIS2 encourages cooperation among member states and EU institutions to develop and promote guidelines and best practices related to cybersecurity, which can include standards that entities should follow.

3.4.4 United Kingdom

The UK has taken steps similar to those taken by the CCCS to provide resources to agri-food operators, and by extension, those across the FVC, aimed at enhancing cybersecurity. For example, the UK's National Cyber Security Centre worked with the National Farmers' Union to develop a producer-focused cybersecurity guide, Cyber Security for Farmers [162], which describes a set of basic cybersecurity practices, not unlike those identified in Canada's Baseline Cyber Security Controls for Small and Medium Organizations [137]. However, the guide does not explicitly link its recommended controls to a specific standards framework. In addition to the guide, the National Cyber Security Centre has also published a suite of resources for small and medium organizations [163], which include:

- Basic cyber awareness guide;
- Free cyber action plan tool for organizations; and
- Small business cybersecurity guide.

In the King's Speech 2024 [164], the UK government signalled its intention to put forward new legislation to strengthen the cybersecurity of CI. The proposed Cyber Security and Resilience Bill [165] will:

- Focus on CI providers, broadening the current network and information security framework [166] to extend protection across digital services and supply chains;
- Mandate ransomware reporting, enabling authorities to better grasp the threat's scale and enhance the capacity to alert affected parties by widening the types of incidents regulated entities are required to report; and
- Grant new powers to regulators and extend the reach of existing regulations.

The EU's NIS Directive was adopted in 2016 to create "a common level of security for network and information systems," and it focuses on network and information systems security and the digital data they hold and transmit, in contrast to the UK's GDPR, which focuses on the processing of personal data [167]. As mentioned in Section 3.2.1, the UK's *Product Security and Telecommunications Infrastructure Act* 2022 [98], which came into effect in 2024, requires that businesses in the supply chains of consumer products that can connect to the internet or a network (e.g., smart surveillance cameras) are compliant with the accompanying legislation that specifies minimum security requirements [168]. These requirements include:

- Meeting minimum password requirements;
- Providing information on reporting security issues to a designated point of contact;
- Providing information on the minimum period during which security updates are provided as part of a product; and
- Adhering to relevant provisions within ETSI EN 303 645 and ISO/IEC 29147 in order to achieve compliance with security requirements [149].

3.4.5 Netherlands

In the Netherlands, the National Cyber Security Centre has been actively facilitating sectoral cooperation to enhance organizational cybersecurity [6]. The Netherlands Cybersecurity Strategy 2022–2028 (NLCS) [170] was developed through collaborative processes involving public, private, and civil society organizations, which were coordinated by the National Coordinator for Counterterrorism and Security, with information provided by the Cybersecurity Threat Assessment for the Netherlands [170]. Given the collaborative, multi-party approach taken in developing the NLCS, the nature of a cyber risk is conceptualized relationally, as the result of an interaction among certain organizational and sectoral interests, threats to those interests, and the organizational cybersecurity practices and levels of cyber resilience relating to the threats. The strategy reflects the need for an integrated approach to cybersecurity and cyber resilience, which relate to [170]:

- A growing "cyber resilience gap" between organizations (Canada Cyber Foundry refers to this as the "cyber poverty line");
- Workforce capacity issues;
- Lack of clarity on responsibilities within the cybersecurity ecosystem;
- Fragmented information sharing across organizations;
- Limited perspectives and information on the nature and scale of harms;
- Immature capacity and practices to enable learning and knowledge sharing about cyber incidents;
- Insufficient research knowledge transfer and marketing of innovation;
- Challenging nature of developing international cybersecurity norms, which means the creation, adoption, and implementation of international norms regarding state responsibility are progressing slowly; and
- Limited cybersecurity awareness and knowledge of cybersecurity best practices among smaller organizations and members of the public.

The NLCS is a values-based document, emphasizing an underlying commitment to the role that digital technologies and digital security can play within a just and equitable society. It embodies a social contract in which digital security is something that everyone can count on. This is reflected in a set of guiding principles for the development of cybersecurity policy and legislation, which include [170]:

- Cybersecurity is integral to the domestic digitalization process.
- Digital security and resilience should be a common good, and cyber risks are shared as part of a broader risk assessment requiring that organizations take proportionate, realistic, and sector-specific measures.
- All relevant organizational and government parties have a responsibility for their own cyber resilience; the role of government is to inform, stimulate, facilitate, and assist based on risk assessment. Government also sets legal and other frameworks, and intervenes where necessary, considering organizational maturity levels and interests of organizations.
- Organizations and the public require clarity on how and when they can seek information, expertise, and assistance.
- Central government and relevant authorities exemplify appropriate levels of resilience to the public interests they must safeguard.
- Government capacity must be deployed efficiently and effectively. The strategy is to serve as the general organizing framework to prevent fragmentation of effort in the cybersecurity domain; specificity can be achieved through sectoral policies, strategies, and roadmaps, including those reflecting emerging norms.
- Public–private partnerships that are accountable for results are foundational to the strategy.
- Because digital security spans national borders, international cooperation is essential. Solutions should seek to strengthen cybersecurity and digital autonomy in an international and European context.

As shown in Table 7, the NLCS is based on four pillars emphasizing resilience, security, response posture, and workforce capacity.

The NLCS includes an explicit acknowledgement of the human, socio-technical dimension of cybersecurity. Moreover, it recognizes the need for agility in responding to shifting threats and opportunities in ways that have not been made explicit in other such frameworks and standards regimes: *The Netherlands' digital security is inextricably linked to technological and social developments. Cybersecurity measures that are effective today might be obsolete by tomorrow, and that is why the government has opted for an adaptive approach to this strategy and the associated action plan. In order to respond to trends, current threats and risks, we need to be able to develop, adjust or intensify the measures arising from the Netherlands Cybersecurity Strategy over time* [170, p. 47]. To this end, monitoring, evaluation, and ongoing learning are identified as necessary components of effective implementation and sustainable value. Although the NLCS does not explicitly mention the agri-FVC, its principle of specificity, its focus on collaboration, and its emphasis on agility in the context of all-of-society capacity, compensate for the lack of a sector-specific framework.

3.4.6 Australia

In 2023, the Australian Ministry for Home Affairs and Cyber Security released its 2023–2030 Australian Cyber Security Strategy [171] to address a legislative gap following the introduction of the Security of Critical Infrastructure Act 2018 [172]. The strategy's implementation is divided into three phases: foundation setting, the development of cyber maturity across the economy, and global leadership in cybersecurity. It also features a multi-layered view of change, including attention to human and technological layers of the cybersecurity ecosystem, which are denoted as the following six "cyber shields" [172]:

- Strong businesses and citizens;
- Safe technology;
- World-class threat sharing and blocking;
- Protected CI;
- Sovereign capabilities; and
- Resilient region and global leadership.

Table 7: The four pillars of the Netherlands Cybersecurity Strategy.

Pillar/Emphasis		Corresponding Aims
1. Cyber resilience of the government, businesses, and civil society organizations	Reduce risks to an acceptable level using a variety of prevention measures. Where incidents occur, promote ability to minimize damage and enable recovery.	Organizations understand threats and risks and how to manage them. Organizations are properly secured against cybersecurity risks and understand their role within an interconnected sector. Organizations are able to respond, recover, and learn from incidents.
2. Secure and innovative digital products and services	Suppliers and consumers of digital products and services Promoting cybersecurity knowledge, development and innovation. Enabling a secure and innovative digital economy contributing to national prosperity.	Digital products and services are more secure. A vigorous domestic cybersecurity knowledge and innovation chain.
3. Counteracting cyber threats posed by states and criminals	National and international approaches to contending with malicious cyber actors based on insights about the cyber threat landscape. A key role for government.	Clarity about cyber threats posed by state and criminal actors. States participate in normative responsible behaviours in cyberspace.
4. Cybersecurity labour market, education, and cyber resilience of the public	The human dimension of cyber resilience. Whole-of-society approach regarding development of digital skills.	Proper protection of the public against cyber risks. Timely public response to cyber incidents. Digital and cybersecurity education in schools. Domestic labour market capacity to address demand for cybersecurity expertise.

The Australian strategy includes regulatory reforms under existing legislation, bringing new attention to cyber incident reporting, ransomware payments, data retention, and corporate governance [171].The strategy also encourages the adoption of international cybersecurity standards for IoT devices through collaboration with industry and international partners to influence the development and adoption of international software security standards by Australian organizations, including secure-by-design and secure-by-default practices [171].Although food and grocery are identified as one of 11 CIs, the strategy does not contain any specific direction about the need or the targeted methods for building cyber preparedness and resilience within this sector.

The Australian Signals Directorate outlined the following eight baseline essential strategies (the "Essential Eight") to mitigate cybersecurity incidents by protecting IT and OT [173]:

- Patch applications;
- Patch operating systems;
- Multi-factor authentication;
- Restrict administrative privileges;
- Application control;
- Restrict Microsoft Office macros;
- User application hardening; and
- Regular backups.

The Essential Eight include a corresponding three-level maturity model to enable organizations to implement cybersecurity controls aligned to their environments and levels of capacity. Table 8 provides an example of the three levels of maturity for one element of the strategy, application control, which refers to the practice of managing and restricting the execution of applications on a system or network. This involves

Table 8: Example of Essential Eight maturity levels for application control.

Level 1	Level 2	Level 3
Application control is implemented on workstations.	Application control is implemented on workstations.	Application control is implemented on workstations.
	Application control is implemented on internet-facing servers.	Application control is implemented on internet-facing servers.
		Application control is implemented on non-internet-facing servers.

allowing only approved applications to run, thereby preventing unauthorized or potentially harmful software from executing. Application control helps mitigate risks by reducing the attack surface, controlling software vulnerabilities, and ensuring compliance with security policies. Where agri-FVCs are diverse in their levels of digitalization and cybersecurity capacity, including a maturity dimension within a future standards framework may be a useful consideration.

The Securing Critical Agriculture Technology and Emerging Solutions research initiative also aims to develop and disseminate user-friendly cybersecurity solutions to agricultural producers [174]. The broader goal of this new initiative is to secure AI and IoT-enabled digital agriculture and address overall sector vulnerability. As mentioned in Section 3.2.1, *Australia's Cyber Security Act 2024* [105] mandates that organizations must report if they paid a ransom. It does not criminalize the payment but mandates the reporting of payment.

3.4.7 New Zealand

New Zealand's National Cyber Security Centre has a function analogous to that of its counterparts in the UK and Canada. In 2024, it released a beta Cyber Security Framework for public feedback [175]. The framework, which consists of five core cybersecurity functions and a corresponding set of desired outcomes, reflects the National Cyber Security Centre's position that cybersecurity "is a multi-dimensional challenge" [175]. The five functions of the framework, which are centred around the first, can be described as follows:

1. Guide and Govern: The promotion of cybersecurity through organizational governance and guidance to staff.
2. Identify and Understand: Knowledge of, and accountability for, the cybersecurity practices relevant to an organization, including asset identification, situational awareness of the business context and its threat environment, and distinguishing between cybersecurity responsibilities internal to the organization and those belonging to suppliers and providers.
3. Prevent and Protect: A practical focus on addressing current risks within an organization's scope of control, while pursuing incremental improvement, through a focus on addressing vulnerabilities and protecting assets.
4. Detect and Contain: Understanding system functions and connections, monitoring, and containing incidents.
5. Respond and Recover: Prioritizing incident response to enable prompt recovery of critical business functions.

Similar to Canada's Baseline Cyber Security Controls for Small and Medium Organizations [137], the New Zealand framework draws from elements of the US NIST Cybersecurity Framework (CSF) [176], [104]. As shown in Table 9, the two frameworks are broadly similar.

The New Zealand framework makes two key modifications to the NIST CSF. First, while the NIST framework outlines 22 categories and over 100

Table 9: Comparison of New Zealand's Cyber Security Framework functions to the NIST Cybersecurity Framework (adapted from [175]).

New Zealand Cyber Security Framework Functions	Corresponding NIST Cybersecurity Framework Functions
Guide and Govern	Identify
Identify and Understand	
Prevent and Protect	Protect
Detect and Contain	Detect
Respond and Recover	Respond
	Recover

subcategories of activities within its five primary functions, the New Zealand framework focuses on defining what successful outcomes look like for each top-level function instead of detailing each activity in a granular fashion [175]. The intent of this is twofold: to make it easier to engage with other agencies using different frameworks, and to demonstrate how cybersecurity activities can fit within the framework. Second, the New Zealand framework separates the guide and govern functions, which the NIST CSF framework generally includes under identify. This is done to maintain a clear distinction between cybersecurity governance and cybersecurity management, as separate functions, typically handled by different parts of an organization.

3.5 Cybersecurity Standards and Frameworks

3.5.1 ISO/IEC 27001, Information Security Management Systems

ISO/IEC 27001, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* [178], is an international cybersecurity standards framework designed to help organizations protect their information assets through a systematic approach to managing sensitive data. It is part of the ISO/IEC 27000 series of standards, which provides comprehensive guidelines for establishing, implementing, maintaining, and continually improving an information security management system. From a compliance perspective, the ISO/IEC 27000 series is intended to help organizations position themselves in relation to existing or emerging regulations [179]. ISO/IEC 27000 describes the overall framework and vocabulary, and the corresponding series includes requirements, controls, guidelines, auditing, and adaptations for specific sectors. ISO/IEC 27001 includes specifications for an information security management system, while ISO/IEC 27002 provides an accompanying set of best practices and control objectives [179]. The series emphasizes the importance of risk assessment, planning and implementation activities, training, continuous monitoring, regular audits, and ongoing improvement to ensure that security measures remain effective and relevant in the face of evolving threats. ISO/IEC 27001 is designed to be flexible and scalable, making it applicable to organizations of all sizes and industries. The potential relevance of this standard to the FVC is that it provides a comprehensive framework for managing information security risks applicable to any organization, including farm and food businesses. Implementing an information security management system can help to protect sensitive data, such as crop data, proprietary farming methods, financial records, and operational information, from threats.

3.5.2 ISO 27701, Privacy Information Management System

ISO 27701, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines* [180], provides guidance for establishing, implementing, maintaining, and continually improving a privacy information management system. It is designed to help organizations comply with global privacy regulations such as the EU GDPR. It should be noted that seven relevant ISO/IEC 27000 series standards, aligned to ISO/IEC 27001, have gone through an adoption process to be recognized as national standards in Canada. These are listed in Table 10. Two additional standards with potential applicability to the FVC are ISO/IEC 27017 [188], which provides guidelines for information security controls applicable to the provision and use of cloud services, and ISO/IEC 27018 [189], which focuses on protecting personal data in cloud and computing environments, some of which are used within the FVC.

3.5.3 NIST Cybersecurity Framework

Initially developed to help organizations within CIs approach cyber preparedness in a systematic way, the NIST CSF [176], [177] is now widely recognized and has been adopted globally across various industries. It offers a flexible and voluntary (non-certification based) approach to improving cybersecurity practices, which may make it suitable for organizations of all sizes and sectors. The NIST CSF is organized around six core functions: Govern, Identify, Protect, Detect, Respond, and Recover. These functions provide a high level, strategic view of the lifecycle of an organization's cybersecurity risk management, from understanding and managing risks to responding to and recovering from cybersecurity incidents. Each function is further divided into categories and subcategories, offering specific outcomes and activities that organizations can implement to strengthen their cybersecurity posture. A proposed enhancement [15] to the NIST Cybersecurity Framework suggests that the functions, Identify to Recover, should be bracketed by "Understand and Plan" and "Review and Learn", respectively, to create a virtuous circle of capacity development. One of the key benefits of the NIST CSF is its adaptability; organizations can customize the framework to align with their unique risk environments, resources, and objectives. The framework also facilitates communication between technical and non-technical parties by providing a common language for discussing cybersecurity risks and controls. A defining feature of the NIST CSF is that cybersecurity measures are appropriate to the level of assessed risk and developmentally appropriate to the user [177].

Table 10: CSA ISO/IEC 27000 Series standards aligned to ISO/IEC 27001.

Standard	Alignment with ISO 27001
CSA ISO/IEC 27006-1 [181]	Supports information security management system certification audit requirements
CSA ISO/IEC 27036-2 [182]	Supplier relationship controls; complements ISO 27001 for supply chain security
CSA ISO/IEC 27035-1 [183]	Incident management principles for Annex A controls
CSA ISO/IEC 27013 [184]	Integrates ISO/IEC 27001 with IT service management
CSA ISO/IEC 27557 [185]	Privacy risk management that integrates with ISO/IEC 27001 information security management system
CSA ISO/IEC 27035-2 [186]	Guidelines for incident response planning; supports ISO 27001 controls
CSA ISO/IEC 27036-1 [187]	Overview for supplier relationship risk under ISO/IEC 27001 information security management system



"Implementation of the OSFI cybersecurity guideline by financial institutions serves the dual purpose of enhancing the cybersecurity resilience of their operations and upholding public confidence in the financial system."

3.5.4 ISA/IEC 62443 Series, Automation and Control Systems Cybersecurity Standards

This set of standards produced by the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) provides a structured framework to strengthen the cybersecurity of industrial automation and control systems (IACS) [190]. Within the FVC, such systems can cover crop data, proprietary farming methods, and a range of operational processes. ISA/IEC 62443 combines best practices, requirements, and processes to evaluate and maintain security, while also integrating day-to-day operations, IT, and process safety [190]. The standards set expectations for asset owners, product suppliers, and service providers to use a risk-based approach, define maturity levels to ensure consistent security practices, and classify five security levels—from no protection to accidental or intentional misuse—to defend against advanced, well-resourced attackers [191]. The ISA/IEC 62443 Series establishes cybersecurity benchmarks across sectors using IACS, including electric power generation and distribution, medical devices, transportation, and various process industries. The series has been endorsed by the United Nations and includes guidance [190] on:

- Establishing shared terms, concepts, and models for all relevant parties involved in control systems cybersecurity;
- Assisting asset owners in identifying the necessary security level to address their specific business and risk requirements;
- Creating a unified set of requirements and a cybersecurity lifecycle methodology for product developers, including a mechanism for certifying products and vendor development processes; and
- Outlining risk assessment processes essential for safeguarding control systems.

The ISA/IEC 62443 Series addresses a range of asset owners, product suppliers, and service providers [192]. While these do not include actors directly involved in the FVC, it has been proposed that these standards could play a helpful role in securing operational technologies in automation and control system components of the FVC [83]. This series is specifically designed for IACS, which parallels the technologies used in digital agriculture equipment and food processing environments.

3.5.5 IEC 62443-1-5 Technical Specification

IEC TS 62443-1-5 is a Technical Specification in the IEC 62443 series, providing implementation guidance for CI [193]. Although this technical specification does not currently include the FVC, guidance for CI operators in settings involving IACS could be examined for applications to FVC processes, such as primary production, manufacturing and processing, distribution, and retail.

3.5.6 Office of the Superintendent of Financial Institutions

The Office of the Superintendent of Financial Institutions (OSFI) [194] is the regulatory body responsible for overseeing federally regulated financial institutions in Canada, including banks, insurance companies, and pension plans. OSFI's guideline on Technology and Cyber Risk Management is designed to enhance the resilience of these institutions against cyber threats and ensure the stability of this CI. OSFI's cybersecurity guidance focuses on risk management practices that institutions must implement to protect their information systems and data. The framework emphasizes the importance of robust governance structures, requiring senior management and boards of directors to be actively involved in cybersecurity oversight. It also mandates federally regulated financial institutions to conduct regular risk assessments, develop and test incident response plans, and continuously monitor and update their cybersecurity controls in response to emerging threats. Key components of OSFI's framework include guidelines on third-party risk management, ensuring that financial institutions assess and manage cybersecurity risks within their supply chains. Additionally, OSFI encourages institutions to adopt industry best practices and align their cybersecurity measures with international standards, such as ISO 27001 and the NIST CSF.

OSFI's Technology and Cyber Risk Management guideline is organized into the following three domains of effective technology management and cyber risk management [194]:

- Governance and risk management: Involves expectations for organizational structures and processes related to leadership, accountability, risk management, and oversight of technology and cybersecurity;
- Technology operations and resilience: Focuses on expectations related to the design, implementation, management, and recovery of technology assets and services; and
- Cybersecurity: Involves expectations regarding the management and oversight of cybersecurity risk, including commitments to continuous improvement and consideration of third-party provider risks. The cyber risk management framework includes the following elements [194]:
  - Accountability for technology and cyber risk management;
  - Technology and cyber risk appetite and measurement;
  - Technology and cyber risk taxonomy;
  - Control domains for technology and cyber security;
  - Policies, standards, and processes governing technology and cyber risk, which are approved, regularly reviewed, and consistently implemented enterprise-wide;
  - Processes for identifying, assessing, managing, monitoring, and reporting on technology and cyber risks, including processes for managing exceptions;
  - Management of unique risks posed by emerging threats and technologies; and
  - Reporting.

Implementation of the OSFI cybersecurity guideline by financial institutions serves the dual purpose of enhancing the cybersecurity resilience of their operations and upholding public confidence in the financial system. This is achieved through protecting customer and organizational data as well as by ensuring the integrity of financial transactions. By taking a proactive approach, the framework seeks to contribute to the overall stability of the financial sector, which has significant implications for public trust and Canadian prosperity and well-being, which are also essential elements of a vital FVC. However, while a shared interest in countering common threats is important, it does not necessarily outweigh the expectations that businesses and citizens have for frictionless access to the internet [195]. Consequently, the Canadian government faces the challenge of striking a balance between implementing the necessary regulations to protect financial system users and fostering easier transactional experiences. For example, the balance between the desire of consumers and businesses for lower transactional friction and the need to safeguard data and privacy is a key tension in the domain of "open banking" [196]. The broader

framing of this cybersecurity guidance to include governance, risk management, and resilience within a CI may help to elevate FVC cybersecurity from single operational perspectives to ones involving enterprise and systemic considerations. Furthermore, addressing FVC cybersecurity through a lens that includes governance and risk management may enable the development of better situational awareness and open planning discussions to the topic of the social contract among various FVC parties.

3.5.7 Hazard Analysis Critical Control Points

The Hazard Analysis Critical Control Points (HACCP) framework is a longstanding and systematic approach to ensuring food safety by identifying, evaluating, and controlling hazards that could compromise the safety of food products (e.g., [197]). In some countries, a HACCP plan is a requirement. In Canada, food businesses (e.g., dairy, retail, food services) are required to have a food safety plan as part of their mandated food safety program under provincial or federal regulation. When audited by a government health inspector, the food safety plan and the business's record-keeping system will be required to demonstrate compliance with relevant standards for food safety [198]. HACCP plans operate on seven core principles [199]:

1. Conduct hazard analysis: Identifying and analyzing potential physical, chemical, biological, or microbiological hazards.
2. Determine critical control points (CCPs): Identifying processing steps where controls can be applied to prevent or reduce health hazards.
3. Establish critical limits: Assigning maximum or minimum allowable limits for CCPs.
4. Establish monitoring procedures: Identifying which parameters should be monitored and specifying procedures to monitor them.
5. Establish corrective actions: Determining specific actions to be taken to return CCPs to safe levels when deviations are detected.
6. Establish verification procedures: Creating plans to verify that the HACCP plan is working effectively and to re-evaluate new or emerging hazards, not originally anticipated within the system.
7. Establish record-keeping and documentation: Maintaining and ensuring adequate storage of the records of all HACCP-related activities to ensure traceability and to support compliance auditing.

The HACCP framework is widely used in the food industry to manage risks, ensure product safety, and comply with regulatory requirements, helping to protect public health by preventing foodborne illnesses. While not originally designed for cybersecurity, the HACCP approach bears similarities to some of the features of cybersecurity standards. The key points of similarity centre on the protection of assets and processes by systematically managing risks and ensuring that critical security measures are consistently maintained. The potential broader relevance of the HACCP framework for the FVC relates to its focus on proactive risk management, which is particularly beneficial in a business context within which cyber threats and cyber threat actors continue to expand and evolve. Exploring opportunities to align relevant cybersecurity practices in the FVC to the food processing sector's approach to food safety could be one tool for enhancing the cybersecurity capacity of the food system while mitigating against digital hazards.

3.5.8 PCI Data Security Standard (DSS), Version 4.0

The PCI Security Standards Council published this standard, known as the PCI DSS v4.0, in March 2022 [200], which is applicable to organizations that handle credit cards payments. It introduces new requirements to address emerging threats and technologies, focusing on security as a continuous process and promoting security as a shared responsibility. This standard could relate to direct-to-consumer farm sales and stores or suppliers that accept credit card payment within the FVC. Although the PCI DSS v4.0 would be expected to figure in supply chain processes involving credit card transactions, the perspective of security as a



continuous process supports a holistic perspective on FVC cybersecurity and resilience. The focus on shared responsibility aligns to the recognition that cybersecurity is a shared risk and a shared responsibility.

3.5.9 System and Organization Controls (SOC) 2 Reports

Developed by the American Institute of Chartered Professional Accountants, SOC 2 reports [201] define criteria for managing customer data based on five "trust service principles": security, availability, processing integrity, confidentiality, and privacy. SOC 2 Type II reports are often required by clients to ensure that service providers securely manage data. SOC 2-based engagements provide details on a service organization's controls in areas related to:

- Overall security of the organization's system related to confidentiality, integrity, and availability; and
- Privacy of personal information that the organization gathers, uses, holds, shares, and disposes.

SOC 2 reports may be relevant to insurance industry needs. Awareness of these principles and practices may support incorporated FVC businesses in meeting various financial audit requirements.

3.5.10 Control Objectives for Information and Related Technologies (COBIT) 2019

Published by the Information Systems Audit and Control Association, COBIT 2019 [202] is a framework for the governance and management of enterprise IT. It provides comprehensive guidelines for designing and implementing enterprise governance of information and technology. Of relevance to the FVC, COBIT 2019 includes attention to third-party risk management. With increasing digital connectivity between vendors and purchasers, such as producers or manufacturers and large retailers, there is a growing need to consider the cybersecurity of all of an organization's digital touchpoints. COBIT 2019 is well aligned to the needs of larger corporate entities. The COBIT case studies, which illustrate the application of the framework to a variety of large corporate and public entities, could be used to inform actions by larger FVC actors (at the time of writing, none of the case studies focus on components of the FVC specifically).

3.5.11 Cybersecurity Maturity Model Certification (CMMC) 2.0

This certification system was developed by the US Department of War (formerly Defense) to enhance cybersecurity practices and protect sensitive

unclassified information [203]. The CMMC seeks to ensure that defence contractors comply with current information protection standards for federal contract information and controlled unclassified information. CMMC 2.0 simplifies the model into three levels of certification, aligning with NIST standards. CMMC 2.0 is not directly relevant outside certain situations involving FVC contractors that supply the Department of War, where the information they hold and transmit is classified as federal contract or controlled unclassified information. It would be more difficult to apply to the diversity of actors and capacities within the FVC.

3.5.12 Internet of Things Security Guidelines (NISTIR 8228, ETSI EN 303 645)

Published by NIST in 2019, the NISTIR 8228 guidelines [204] focus on considerations that may impact cybersecurity and privacy risks related to the use of IoT devices as distinct from conventional IT devices. The focus of these high level guidelines is on protecting device-level security, data security, and privacy. The European Telecommunications Standards Institute (ETSI) Consumer IoT Security Road Map, ETSI EN 303 645 [169], was developed as a result of collaboration and knowledge sharing among relevant industry, academic, and government parties, and is designed to prevent widespread attacks on interconnected IoT smart devices used by consumers. The ETSI roadmap was established to enable a security baseline for connected consumer products and to lay the groundwork for future IoT certification programs. This emphasizes incorporating security into IoT products by design. ETSI EN 303 645 includes the following 13 recommendations for achieving a practical level of baseline cybersecurity [169]:

- Examine system telemetry data;
- Make it easy for users to delete data;
- Make installation and maintenance of devices easy;
- Validate input data;
- Make systems resilient to outages;
- No universal default passwords;
- Implement a means to manage reports of vulnerabilities;
- Keep software updated;
- Securely store sensitive security parameters;
- Ensure that personal data is secure;
- Ensure software integrity;
- Minimize exposed attack surfaces; and
- Communicate securely.

The primary audience for NISTR 8228 are US federal personnel responsible for managing cybersecurity and privacy risks for IoT devices. The audience for ETSI EN 303 645 is primarily European manufacturers of consumer-grade IoT devices. The 13 recommendations in ETSI EN 303 645, and its focus on security-by-design, are likely to be useful to the diversity of parties within the FVC.

3.5.13 Federal Risk and Authorization Management Program (FedRAMP)

This is a US government-wide program [205] that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP aims to ensure that cloud services used by federal agencies meet strict security requirements. It can be applied by vendors and service providers with cloud-based solutions and as information for FVC actors purchasing equipment or services. This could potentially be useful as input to the cloud-based elements of FVC components.

3.5.14 Center for Internet Security (CIS) Critical Security Controls Version 8

The CIS Critical Security Controls framework consists of a set of prioritized cybersecurity best practices designed to help organizations improve their cyber defence capabilities. Version 8, released in May 2024 [149], integrates and aligns with many of the previously mentioned cybersecurity standards and guidelines, as well as others. Although this framework is of potential relevance to FVC parties, it does not offer a unique value proposition compared to other standards and frameworks.

3.5.15 Comparison of Standards

The standards and frameworks discussed in sections 3.5.1 through 3.5.14 contain elements that align to key principles within the national frameworks and guidelines reviewed in sections 3.3 and 3.4, as well as design features that could be important to the creation of a successful cybersecurity standards framework for the Canadian FVC. For applications such as digital agriculture and advanced food processing, which rely on interconnected devices, IoT sensors, IACS, and data analytics, several cybersecurity frameworks may be relevant. Some of the most important features of these standards include:

- Integration of technology: Digital agriculture, for example, integrates various technologies that are susceptible to diverse cyber threats.
- Data sensitivity: Agricultural and food sector business data can include proprietary information, trade secrets, and personal data, necessitating robust security measures.
- Operational continuity: Cyberattacks on agricultural and food systems can disrupt operations, leading to financial losses and potential food security issues.
- Regulatory compliance: Adherence to relevant standards helps to fulfill legal and contractual obligations. It also builds trust with relevant parties, strengthening the social contract and climate for innovation and technology adoption.
- Role-based expectations: Covering asset owners, suppliers, and service providers.
- Consideration of maturity levels and use of risk-based approaches: To better, and more holistically, serve the needs and objectives across a variety of organizational settings.

An overview of the potential value of the most promising cybersecurity frameworks is presented in Table 11, which summarizes the general pros and cons of selected frameworks for use within the FVC.

Selecting the right cybersecurity standard involves balancing resource constraints, organizational needs, and the expectations of relevant parties. For the FVC, using multiple standards and guidelines may provide the most comprehensive security approach. For example, standards such as ISO/IEC 27001 and IEC 62443 are comprehensive, but were designed with traditional IT environments and industrial settings in mind. They may not adequately address the unique characteristics of agricultural operations, such as the deployment of IoT devices across vast, remote, and outdoor areas, which are more susceptible to physical tampering, theft, and environmental challenges. These standards often overlook the constraints of agricultural IoT devices, including limited processing power, energy resources, and intermittent connectivity, which can impede the implementation of robust security measures such as encryption and timely updates. Standardization initiatives would also benefit from strengthened attention to the importance of dynamic risk management and resilience, which emphasizes preparing for, adapting to, and being able to continue despite disruptions [206].

With these considerations in mind, the following set of six design features are proposed to guide the development of FVC-specific cybersecurity standards:

1. Applicability: Standards or guidelines must address a wide range of cybersecurity threats, such as ransomware, advanced persistent threats, and the increasingly prevalent issue of social engineering via synthetic media (i.e., deepfake video and audio). They should apply across all OSI layers, ensuring full system protection, and they should anticipate future risks. Comprehensive coverage ensures that no OSI layer is left vulnerable, from physical networking hardware to the application layer, where user interactions occur. As malicious exploits targeting OT have also begun to be identified, it will be important to consider the cybersecurity of both OT and IT components of cyber-physical systems.
2. Relevance: Standards must meet the needs of a wide range of users. They must support both experts and non-experts and allow for gradual improvement over time. In addition, standards must accommodate organizations at various stages of cybersecurity maturity, supporting a collective defence-in-depth strategy. Moreover, they should provide a clear developmental pathway for organizations, allowing for incremental improvements that encourage ongoing engagement and adaptation by users at all levels of expertise.

Table 11: Summary of selected cybersecurity standards and frameworks of potential value to the FVC.

Standard/Framework	Pros	Cons
ISO/IEC 27001	**Comprehensive framework:** Provides a holistic approach to managing information security risks. **Globally recognized:** Enhances credibility and trust with relevant interested parties. **Certifiable:** Offers formal certification to demonstrate commitment to security. **Flexible application:** Can be tailored to any organization, including those in agriculture.	**Resource intensive:** Implementation can be costly and time-consuming. **Generic approach:** Not specific to digital agriculture; may require significant adaptation. **Complex documentation:** Involves extensive paperwork and maintenance.
ISO/IEC 27017 and ISO/IEC 27018	**Cloud security focused:** Addresses specific risks associated with cloud services used in digital agriculture. **Data protection:** Enhances privacy and security of data stored in the cloud. **Extends ISO 27001:** Builds on existing information security management systems.	**Limited scope:** Focuses on cloud services; may not cover on-site devices and networks. **Requires ISO 27001:** Not standalone; dependent on implementing ISO 27001 first. **Additional cost:** May increase overall implementation expenses.
NIST	**Flexible and adaptable:** Suitable for organizations of any size and sector. **Risk-based approach:** Focuses on managing and reducing cybersecurity risks. **Free resource:** Publicly available without cost. **Widely adopted:** Respected framework with extensive support materials.	**US-centric:** Developed by a US agency; may need adjustments for application in Canada. **Non-certifiable:** Lacks formal certification, which may be less persuasive to some parties. **Broad scope:** May require additional industry-specific guidelines for agriculture.
ISA/IEC 62443 Series	**Industry specific:** Tailored for IACS, relevant to agricultural machinery and food processing equipment. **Comprehensive coverage:** Addresses security at all system levels. **Vendor guidance:** Includes requirements for product suppliers and system integrators.	**Complexity:** Series consists of multiple detailed parts, which can be challenging to navigate. **Less known globally:** May not be as recognized outside industrial sectors. **Specialized expertise required:** Implementation may require industrial cybersecurity professionals.
OFSI	**Widely adopted:** Tailored to needs of the financial services industry as a CI. **Financial transactions:** Relevant to financial dimension of FVC businesses, and may have some transferable benefits with respect to other non-financial transactional processes within FVC	**Limited scope:** Focuses on financial industry and its systems.
HACCP	**Originates in FVC:** Developed for food processing environments. **Widely adopted:** Respected framework with extensive support materials. Incorporated into government regulation. **Risk management:** Focus on proactive risk management. **Governance:** Attention to governance issues, which may support social contract among FVC actors.	**Limited scope:** Focuses on food safety aspects of food processing.
IoT Security Guidelines	**IoT specific:** Directly addresses security of IoT devices used in digital agriculture and food processing or logistics applications. **Practical recommendations:** Offers actionable advice for securing devices and data. **Enhances device security:** Helps mitigate risks unique to IoT ecosystems.	**Guidelines, not standards:** No formal certification; may lack recognized authority. **Limited scope:** Focused on devices, not overall system security. **Varied adoption:** May not be universally recognized or enforced.
IEC TS 62443-1-5	**Implementation guidance:** For applying security profiles to IACS, especially in CI. **Potentially broad applicability:** Across IACS within FVC operational settings involving holistic attention to people, processes, and technology.	**Guidelines, not standards:** Have not yet been instituted as normative requirements. **Limited scope:** Focused on IACS, not yet applied to food CI.

3. Technical capacity and affordability: This refers to the ability of organizations to implement and maintain the standards. Support must be accessible and affordable, especially for smaller operations. Determining the technical and financial capacity required to implement and monitor the standards is crucial. This includes an assessment of the resources needed to effectively adopt, use, and evaluate the standards within an organization and across the FVC. Support structures must be robust, readily accessible, and must not impose undue financial burdens on organizations, ensuring that smaller entities can adopt critical standards without prohibitive costs.
4. Agility: In order to adapt quickly to new cyber threats, the standards must be flexible and easy to update. This adaptability will ensure that the standards remain effective and relevant, safeguarding the sector against current and future cyber threats.
5. Shared development: Standards must be developed with input from many groups, including industry, academia, regulators, technology experts, industry members (e.g., producers, agri-business, and food business parties), and technology developers. Non-traditional parties should also be included in this process. This collaborative approach will not only enrich the framework with a diversity of insights but it will also foster a sense of the possible through relevance, ownership, and commitment to the standards across the sector.
6. Context: Standards should be tailored to the FVC while considering the broader impacts, which reflects how cyber threats affect both the sector and society. This involves understanding the interconnectedness of the FVC sector with other CIs and the potential societal impacts of cyber threats in the sector. By drawing attention to these relationships, standards will not only address immediate security needs but will also contribute to a broader understanding of, and preparedness against, wider cybersecurity threats.

In Table 12, six of the previously discussed standards frameworks are compared with the six proposed design features. Of the frameworks analyzed against the proposed design features, NIST offers the most flexibility as a foundation for developing a holistic, yet agile, cybersecurity framework for the FVC that is anchored to a developmental cyber maturity approach.

3.6 Exploratory Survey of Food Value Chain Actors

3.6.1 Survey Respondents

A total of 96 individuals self-selected to respond to the online survey between December 20, 2024 and March 7, 2025. The majority were anglophone (n = 89) and the remainder were francophone (n = 7). Respondents' businesses represented every province in Canada and spanned the FVC. Upstream actors included equipment manufacturers and input suppliers. Downstream actors included food processers and retailers. However, most of the respondents were primary producers or service providers. Service providers, as a lumped category, included financial, insurance, agronomic, IT/cybersecurity, and so on (Figure 6).

3.6.1.1 Familiarity with Cybersecurity Concepts

When asked how familiar they were with cybersecurity concepts, most survey respondents reported they were either "very familiar" or "somewhat familiar" (Figure 7). Given that respondents were self-selected, these results are not necessarily representative of a broader trend. Although it is not possible to determine whether these findings reflect statistically significant differences, it should be noted that, among the different FVC actors, primary producers lag in self-reported cybersecurity awareness. Of those who indicated they are not familiar with cybersecurity concepts, 75% identified as primary producers (see Figure 7). However, 45% percent of those who said they were somewhat familiar also identified as primary producers, signifying that there is some awareness among this group. These findings suggest that there has not been an improvement in cybersecurity awareness among primary producers over what was observed in a 2021 producer survey [5]. Service providers were the most likely to respond as being very familiar with cybersecurity concepts. This is perhaps because service providers included financial, insurance, and IT/cybersecurity services, all of which work daily with sensitive information, necessitating greater cybersecurity literacy for business operations and legal compliance.

Table 12: Comparison of existing standards/frameworks with proposed design features for creating cybersecurity standards for the FVC.

Standard/ Framework	Design Features					
	Applicability	Relevance	Technical Capacity and Affordability	Agility	Shared Development	Context
ISO/IEC 27001	Applicable to a range of emerging risks. The ISO infrastructure is less amenable to a restricted set of controls that may be manageable for small and medium organizations.	The level of technical detail in this framework may not address the more basic cybersecurity needs of the broader population of FVC actors.	A higher level of organizational cyber maturity is necessary for adoption of the ISO framework.	The ISO infrastructure and renewal cycle may not be able to keep pace with the evolving technologies and threat environment confronting digital agriculture. More research on this topic would be required to support a firm assessment.	The collaborative international development and updating of ISO standards presents an opportunity to develop a subset of food sector-specific standards that reflect a diversity of interests. However, influential geopolitical interests may dominate process in ways that could disadvantage relevant Canadian FVC parties. This is a developing issue to monitor carefully.	Attention to the context of the business.
NIST	Applicable to a range of emerging risks. The higher level NIST functions are amenable to a restricted set of controls that may be manageable for small and medium organizations.	NIST is inherently a developmental framework. Its adaptation to the needs of national frameworks and to Canada's Baseline Cyber Security Controls suggests broad applicability.	A condensed set of controls, linked to the most prevalent and emergent threats, could be managed by smaller businesses if a network of affordable services and supports (including training) is available.	The deployment of elements of the NIST framework within national frameworks that also include evaluation components promises to provide a stream of information to support flexible use.	The Netherlands Cybersecurity Strategy exemplifies a commitment to broad engagement of relevant interested parties in a collaborative process of standards development, implementation, and evaluation. This may suggest practical and effective options for the Canadian context.	As used in the national cybersecurity frameworks developed by Australia, New Zealand, and the Netherlands, there is an opportunity to marry elements of the framework to key sectoral and all-of-society considerations.
ISA/IEC 62443 Series	Limited to larger corporate entities outside of agricultural production.	Potentially more immediate applicability to transportation and distribution components, sensor manufacturers, and processors.	May require a higher level of maturity than is present among most small and medium businesses.	The standards in this series follow a five-year update cycle.	Developed collaboratively by ISA and IEC.	Industrial sector organizations, including energy, medical technologies, transportation, and building automation.
OFSI	The domains of technology and cyber risk management are applicable to FVC organizations. Emerging work on open banking may become increasingly relevant for the FVC.	The specifics within each domain are more focused on the needs of this highly regulated sector.	At present, there is insufficient information to support an assessment.	The financial services sector must strive for agility, as one of the most targeted CIs. However, the specific needs of this sector may not always match those of the FVC.	At present, there is insufficient information to support an assessment.	Significant attention to a broad and complex risk environment.
HACCP	The framework's focus on reducing the risk of food borne disease may limit its perceived utility across a broader range of applications within the FVC.	The specifics within each domain are more focused on the needs of this highly regulated sector.]Familiarity with the core principles within components of the FVC, and their alignment with general concepts of cyber risk management, may create opportunities for effective communication in support of cyber practice enhancements.	Food safety training infrastructure could be leveraged to expand its focus on the cybersecurity dimension of risk management and compliance.	At present, there is insufficient information to support an assessment.	At present, there is insufficient information to support an assessment.	More narrow view of food safety.
IEC TS 62443-1-5	Widespread use of IACS across FVC.	Holistic consideration of people, processes, and technology, including a range of actors.	Lends itself to varying maturity levels within a risk management framework. At present, there is insufficient information to support a more fulsome assessment.	This is the result of a development process spanning two decades. Process may not involve sufficient agility to cope with rapidly emerging threats, but may enable holistic and maturity-based attention to cybersecurity across a wide range of FVC actors.	Usual ISA/IEC processes.	May have widespread value in supporting enhanced cybersecurity not just within the food CI, but across intersecting CIs impacting the FVC.

Figure 6: Respondents' role within FVC and location of business (some businesses spanned more than one province).

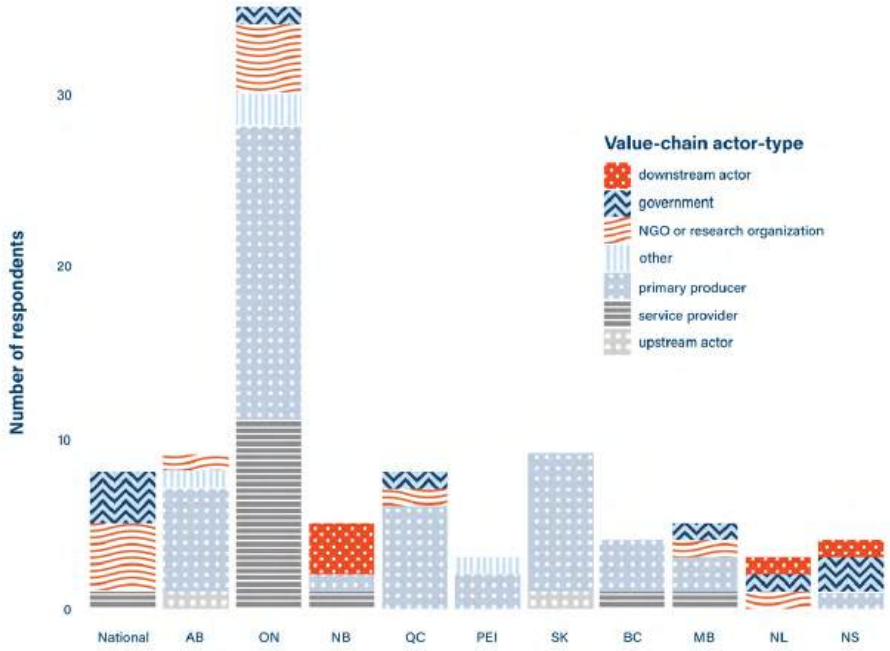
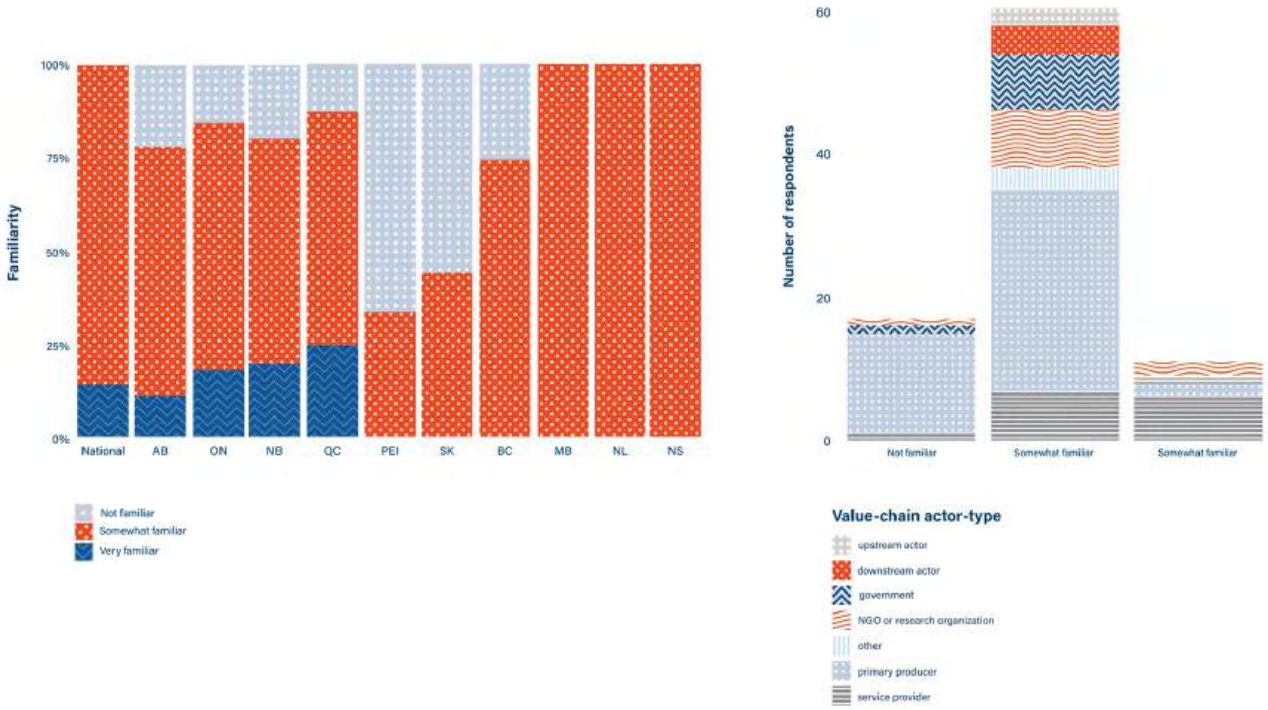


Figure 7: Reported familiarity with cybersecurity concepts by province and by FVC actor.



When asked how they perceived the levels of cybersecurity awareness among peers within their own sector, the majority indicated their peers had some awareness, with many reporting moderate awareness (see Figure 8 and Figure 9). This suggests that the common belief that cybersecurity is entirely overlooked may be misplaced; even modest awareness could serve as a foundation for building a shared sense of urgency around cybersecurity risk management across the FVC.

3.6.1.2 Risk Perception

Most respondents (97.6%) believed that it is likely the FVC will experience a cybersecurity incident within the next few years, and over half believed it is extremely likely. In other words, respondents view a serious cybersecurity event as an eventuality. To add to the evidence that there is a high level of concern about a cybersecurity threat impacting the FVC, almost 90% of respondents indicated that they believe there is a moderate, high, or extremely high level of cyber risk facing the FVC right now (Figure 10). When asked how much of a priority cybersecurity should be for the FVC, the majority of respondents (98%) indicated it should be a priority. However, they also indicated that they do not believe it is currently seen as a high priority for the FVC (Figure 11). When asked to consider cybersecurity readiness across the FVC, respondents rated it as moderate to poor. They indicated that the technologies that need the most attention to cybersecurity are business management software and precision equipment (Figure 12).

While the results are affected by the over-representation of primary producers in the survey sample, it is noteworthy that business management software was identified as the area most in need of attention, well ahead of precision equipment. Although respondents were self-selected—and likely more knowledgeable about cybersecurity than the average actor in the FVC—their concerns align with findings from the literature review. Specifically, they highlighted perceptions that:

- The FVC is at risk of cybersecurity incidents;
- The sector's overall level of cybersecurity readiness remains low; and
- Addressing cybersecurity vulnerabilities is currently a low priority within their respective sectors.

3.6.2 Most Urgent Threats and Vulnerabilities

Respondents identified the most common forms of malicious cyber exploits, ransomware, direct infiltration, and software problems, as the most likely sources of external cybersecurity threats. They also recognized insufficient training as an important focus of building cyber preparedness within the FVC. Although they viewed financial losses to individual businesses as one of the most serious impacts of cybersecurity disruptions, this came second to the concern for broader, systemic impacts on the supply chain as a whole. Similarly, a concern for data-related losses at the level of individual businesses was associated with a corresponding level of concern for the potential impact of cyber events on food safety.

3.6.2.1 Threats Seen as Most Likely to Cause Harm

Respondents who reported a high level of familiarity with cybersecurity concepts identified ransomware attacks, third-party infiltration, and invalidation and compliance (using fabricated data to disrupt valid certification of a process or transmission) as the top cybersecurity threats facing the FVC (Figure 13). When asked about the most serious potential impacts of such threats and vulnerabilities, their leading concerns included supply chain disruptions that could limit consumer access to food, and financial losses stemming from ransom payments, system repairs, or downtime-related revenue loss. Food safety risk, resulting from compromised automated systems, and data theft were also cited as significant potential consequences of a cybersecurity breach (Figure 13).

3.6.2.2 Most Significant Vulnerabilities

This same group of respondents largely agreed that the top priorities for remediating FVC cybersecurity vulnerabilities were insufficient employee training and updating outdated software (Figure 14). This is consistent with the view that business management software is the technology requiring the most urgent attention from a cybersecurity perspective (see Figure 12). However, none of the respondents selected insufficient defences against malicious software (malware), inadequate data encryption, or remote access vulnerabilities (weak protections for remote systems, such as unsecured remote connections) as important vulnerabilities.

Figure 8: Respondents' perceptions of cybersecurity awareness among peers in their sector.

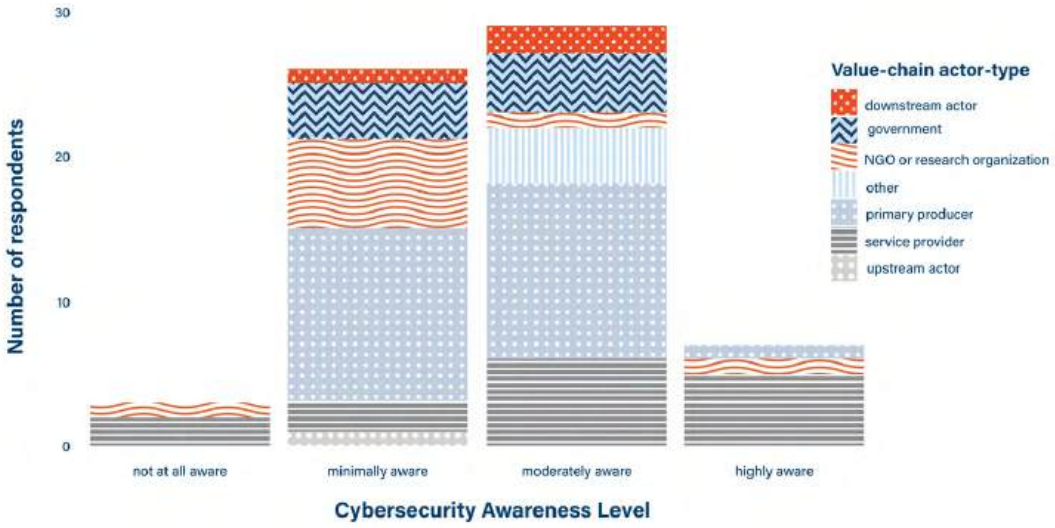


Figure 9: Perceptions of peers' awareness of cybersecurity risk.

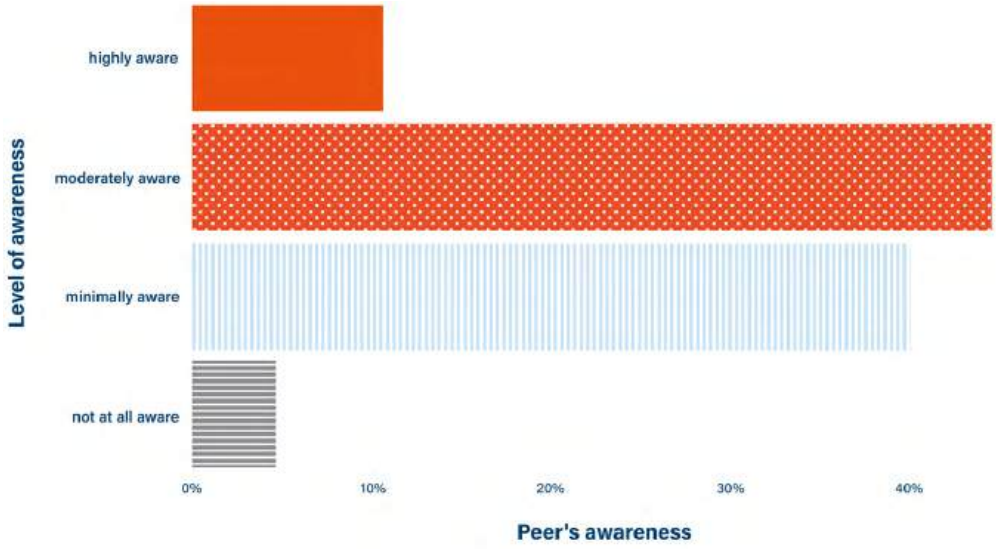


Figure 10: Perceived likelihood of a malicious cyber event affecting the FVC over the next several years and rating of level of current cybersecurity risk.

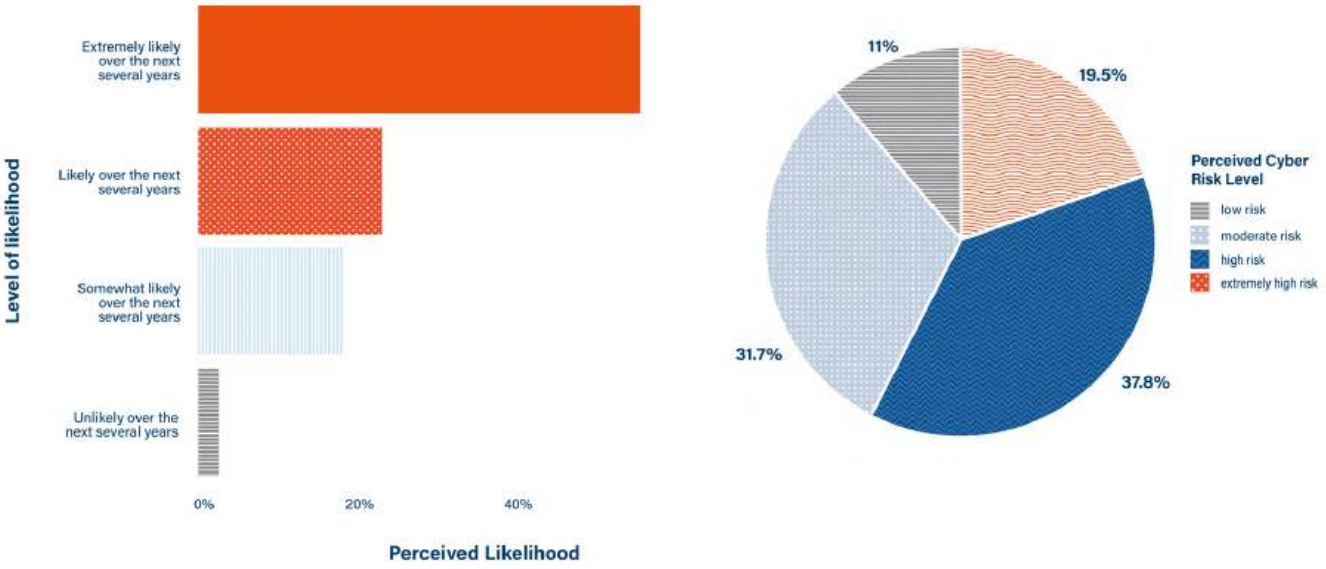


Figure 11: Belief about how much of a priority cybersecurity in the FVC should be versus belief about how much of a priority it is seen as currently.

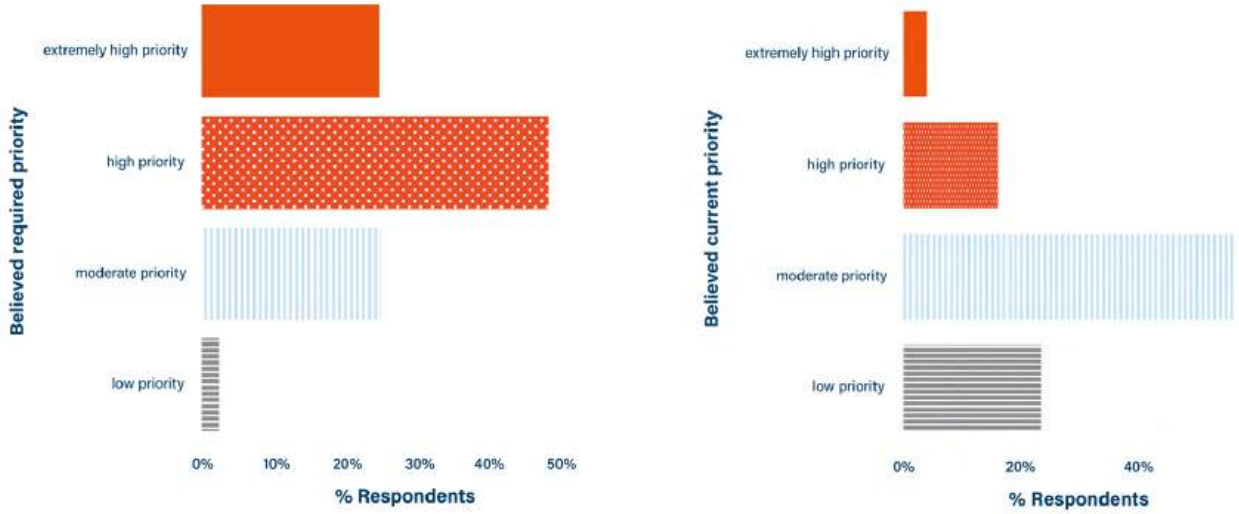


Figure 12: Perceptions of cybersecurity readiness across the FVC and identification of technologies needing the most attention.

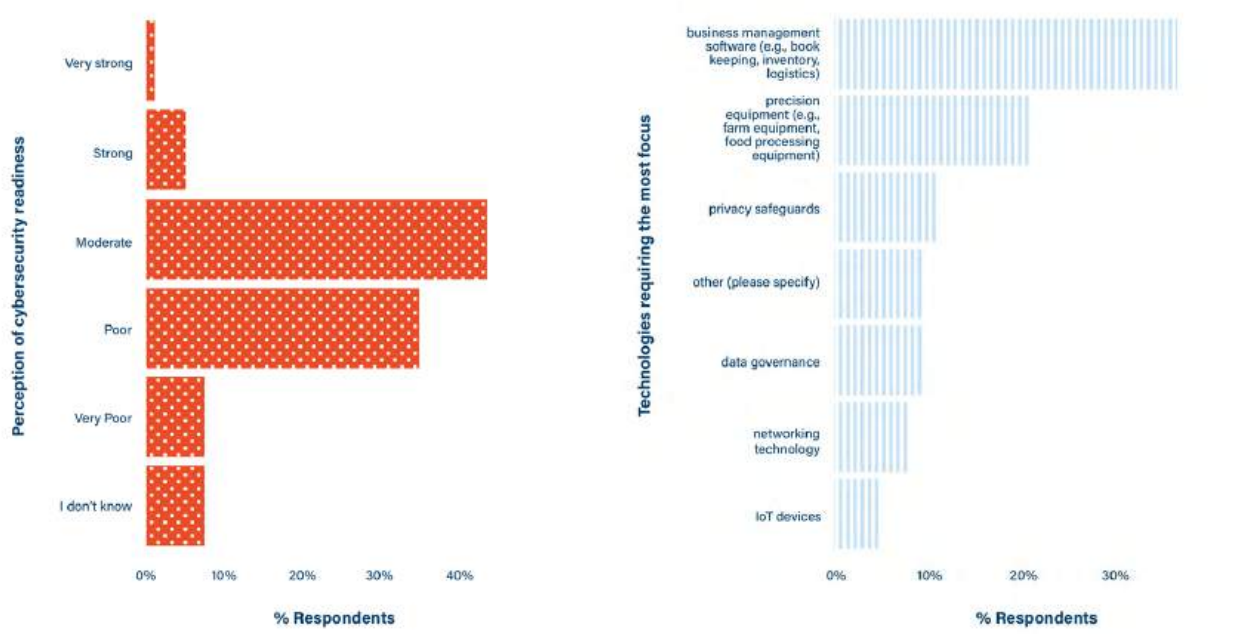


Figure 13: Most frequently endorsed cybersecurity threats and impacts.

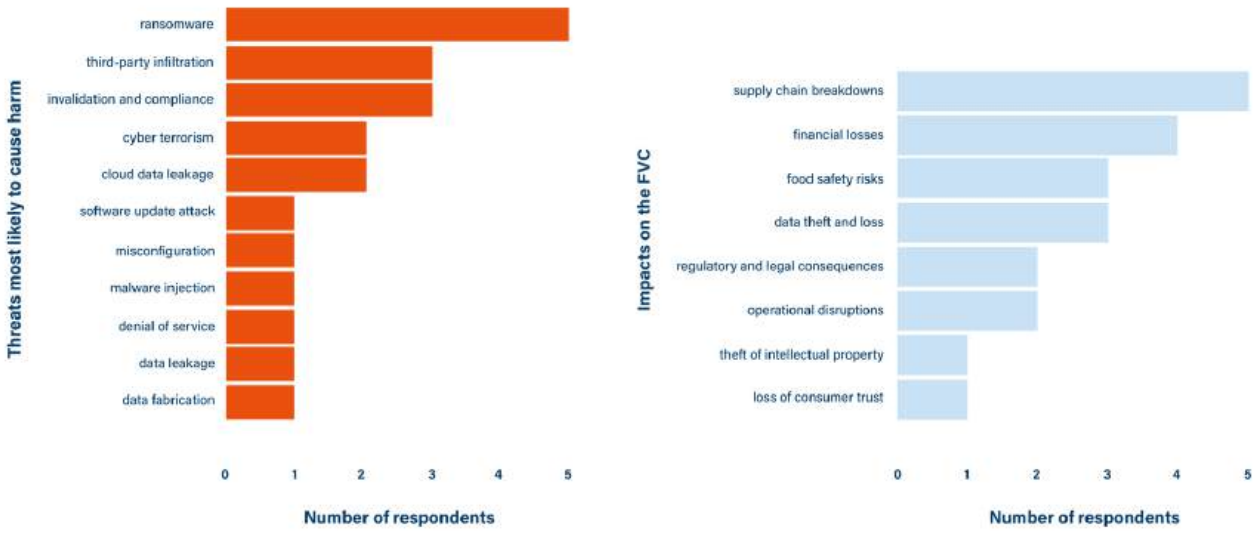
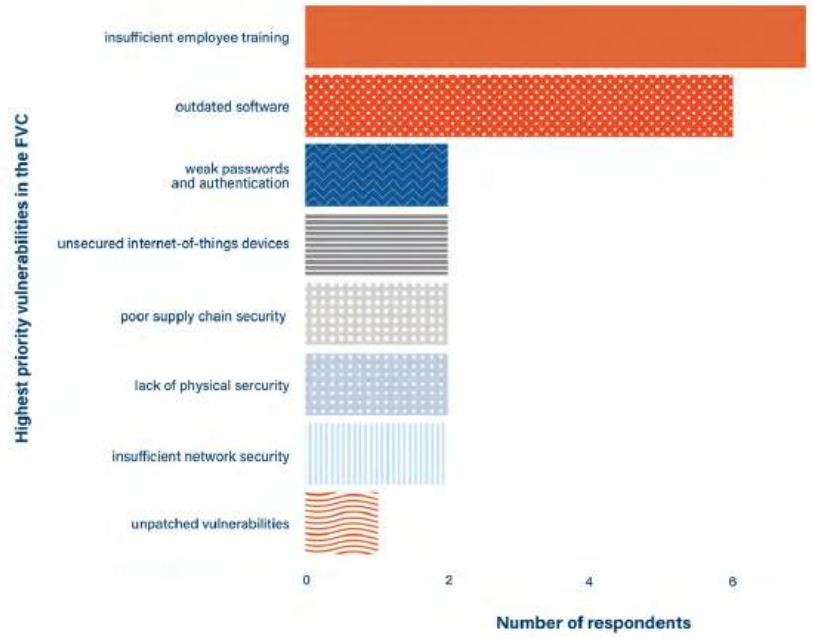


Figure 14: Cyber vulnerabilities.



Thinking about the most urgent threats and vulnerabilities confronting the FVC, respondents noted that these risks involve a range of human, technological, and systemic factors and impacts:

- Employee awareness and training, along with outdated software, were identified as the key vulnerabilities.
- Ransomware, third-party infiltration, and compliance failures were identified as the top threats. Cyber terrorism and cloud data leakage were also identified.
- Participants believed these vulnerabilities and threats could lead to significant consequences, including supply chain disruptions, financial losses, food safety risks, and the theft or loss of data.

3.6.3 Advancing Cybersecurity and Standards in the Food Value Chain

3.6.3.1 Awareness of Cybersecurity Standards

While respondents identified numerous areas of the FVC where cybersecurity standards might currently be in use, over 30% indicated that they were not aware of any such standards being used in any area of the FVC (Figure 15). Participants were asked if they were aware of specific cybersecurity standards that might be applicable to the FVC. Over 40% were not familiar with any standard frameworks that might be relevant.

Among standards frameworks, ISO/IEC 27001 and NIST were the most frequently identified. Although ISO/IEC 27017 and 27018 and the IoT Security Guidelines (NISTIR 8228 and ETSI EN 303 645) were also identified, the HACCP framework for food safety, which is not a cybersecurity framework, was identified more frequently (Figure 16).

Survey findings suggest that awareness of cybersecurity efforts and standards within the FVC remains limited, with many participants unable to identify any standards in use. Among those who could, ISO/IEC 27001 and NIST were the most frequently cited. When respondents who had identified a standard were asked about its potential shortcomings in the FVC context, only two indicated that the standard fell short: one noted that ISO/IEC 27001 lacks industry specific context, and another suggested that the NIST standards are too complex and costly to implement. When asked about the primary focus of the cybersecurity standards in use, nearly half of those responding selected all available options, which indicates that the respondents who were aware of these frameworks understood them as providing broad cybersecurity benefits and overall cyber hygiene rather than serving a single, narrow purpose, even as general awareness of entities working to advance cybersecurity within the FVC remains low.

Figure 15: Areas of the FVC in which respondents indicated that cybersecurity standards may be in use.

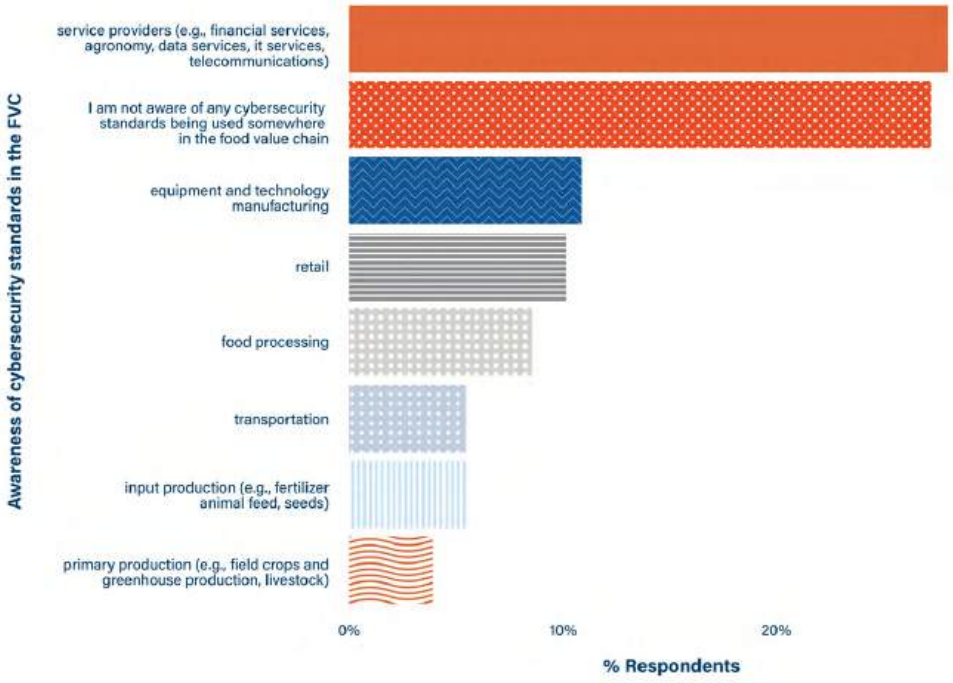
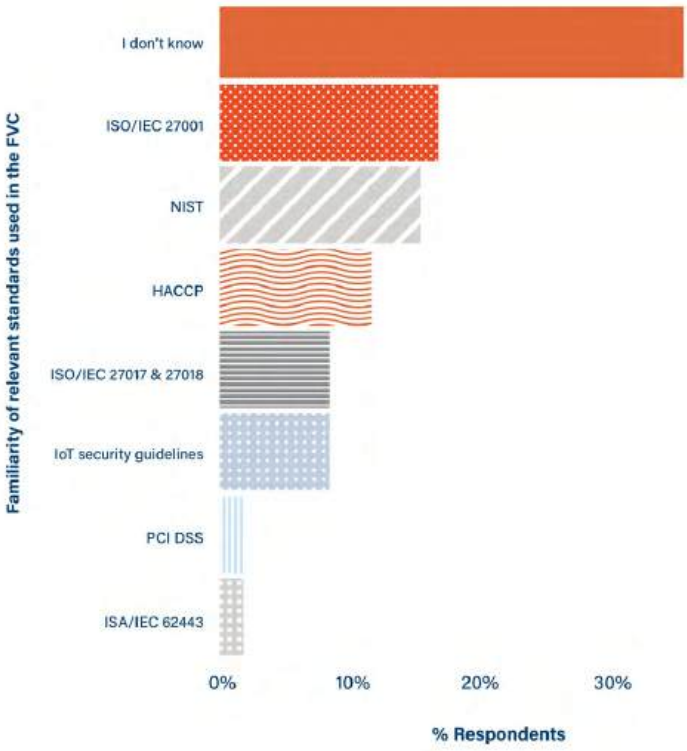


Figure 16: Cybersecurity standards that might be applicable to the FVC.



3.6.4 Views on the Potential Role for Cybersecurity and Standards in the Food Value Chain

3.6.4.1 Potential Benefits

In addition to yielding benefits for the overall cybersecurity posture of an organization, respondents indicated that there were many potential benefits of cybersecurity standards within the FVC (Figure 17). Interestingly, half of these involved human and relational benefits, such as enhanced collaboration, relevant interested party awareness, improved incident response capacity, facilitating technology adoption, and building consumer trust. When asked which components of the FVC could benefit most from cybersecurity standards, participants identified service providers, equipment and technology manufacturers, and food processors. This likely reflects the fact that the first two often handle sensitive information, such as financial or operational data (e.g., yield data), while food processors face significant food safety risks and potential harm if a cybersecurity incident were to impact automated systems (Figure 18).

3.6.4.2 The Potential for Cybersecurity Standards Specific to the Food Value Chain

Survey respondents overwhelmingly endorsed the value of having cybersecurity standards tailored to the specific needs of the FVC (Figure 19). Respondents also emphasized that cybersecurity standards should be more heavily weighted toward the Canadian context rather than being internationally focused (Figure 20). It should be noted that these responses were provided during a period when significant trade tariffs were being imposed on Canada by the US, along with threats to annex the country. Consequently, survey responses may reflect a more protectionist viewpoint designed to strengthen Canadian sovereignty, as much as substantive technical and operational concerns.

Among participants who identified as being very familiar with cybersecurity concepts, their top priority for cybersecurity standards was employee training and awareness. This was followed closely by several priorities in second-place: supply chain security, securing IoT devices, data protection and privacy, and access control and authentication. Network security and incident response and recovery were identified as the third highest priorities. Few participants selected system and software updates, physical security, or risk assessment and management. When asked what the top barriers might be to developing cybersecurity standards for the FVC, participants identified lack of awareness and understanding among FVC parties, and resource constraints as the top two potential barriers. Other potential barriers included competing priorities that may overshadow the perceived need for investments in cybersecurity capacity. When respondents were asked to identify all of the elements that would have to be in place to support the effective use of cybersecurity standards, the most frequently endorsed were education and training programs, clear guidelines and documentation, adequate funding, support and resources, and technical support and expertise (Figure 21).

In addition to these features, respondents also suggested that any approach to developing and implementing cybersecurity standards within the FVC would need to be comprehensive and should include outreach or extension components. Other comments emphasized the need for independent, certified, compliance auditors and a circumscribed role for government, which may include carefully calibrated incentives for compliance and penalties for non-compliance. When asked what other types of supports would help in the development of improved cybersecurity capacity if FVC-specific standards were not available, the most frequently endorsed options were cybersecurity awareness and training, financial incentives, and cybersecurity guidelines for the FVC that are based on existing standards (Figure 22).

Respondents' perspectives on the value, focus, and implementation priorities of cybersecurity standards tailored to the FVC reflected support for sector-specific guidance, particularly to strengthen security practices in an underprepared sector, and emphasized the importance of a Canadian context, employee training, and complementary tools such as guidelines and outreach. Participants identified several potential benefits of having cybersecurity standards specific to the FVC, with the most important being the improvement of overall security practices in a sector

that is underprepared compared to other CIs. All components of the FVC were seen as potentially benefitting from sector-specific standards. However, respondents identified agri-food service providers, food processors, and equipment and technology manufacturers as the actors for which cybersecurity standards would yield the greatest overall benefit. Based on this, if FVC-specific cybersecurity standards were to be developed, it would be important for them to reflect a balance between Canada-focused and internationally-focused considerations, with a greater emphasis on the Canadian context. Employee training and awareness were identified as critical for the future development and implementation of cybersecurity standards for the FVC. In the absence of FVC-specific cybersecurity standards, cybersecurity guidelines for the FVC that are based on existing standards were seen as beneficial to the sector's overall cybersecurity posture, along with awareness and outreach and incentives for practice enhancements.

3.6.5 Governance and Leadership in the Development of Cybersecurity Standards for the Food Value Chain

The survey also engaged respondents on the topic of who should drive support for cybersecurity standards development within the FVC, emphasizing the importance of industry leadership, broad collaboration, and a supportive role for government.

3.6.5.1 Who Should Lead?

When respondents were asked which top three groups they believed were best positioned to provide leadership on making the FVC more cybersecure, their answers suggested an important role for cross-cutting actors within the FVC (i.e., equipment and technology providers: 15%; NGOs: 15%; government: 15%; service providers: 30%; food processors: 12%; primary producers: 8%; input suppliers: 4%) (Figure 23).

Figure 17: Potential benefits of widespread adoption of cybersecurity standards within the FVC

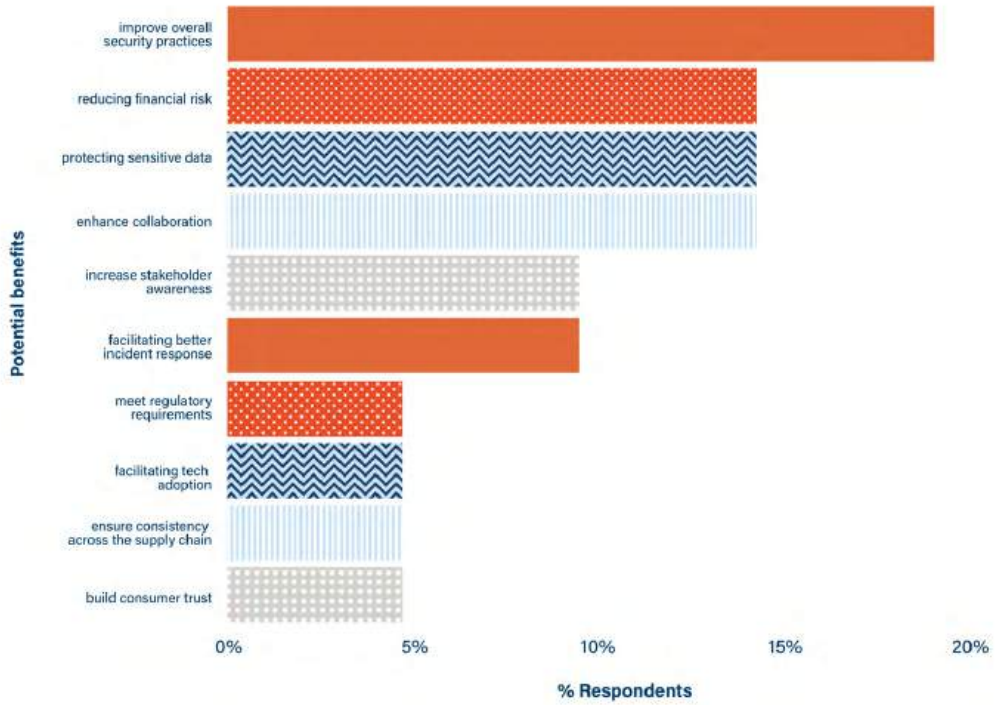


Figure 18: Areas of the FVC that stand to benefit most from cybersecurity standards.

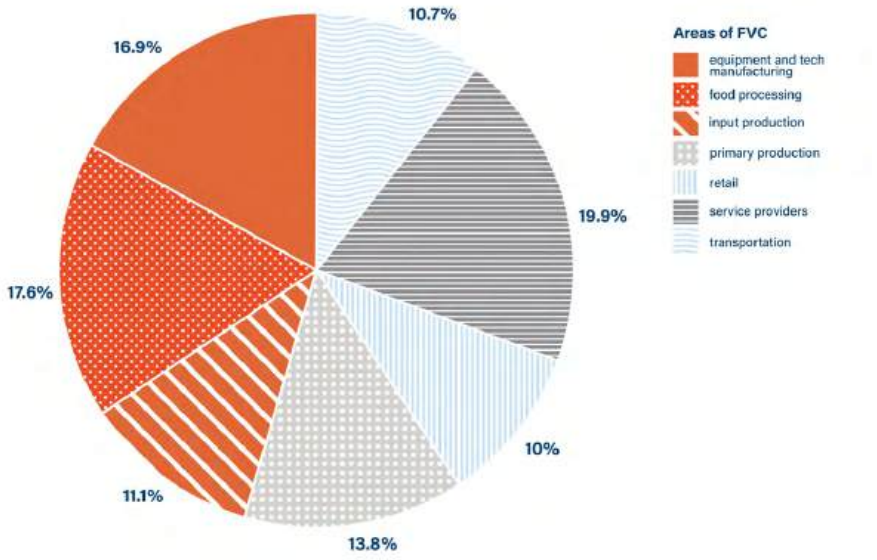


Figure 19: Importance of having cybersecurity standards specific to the FVC.

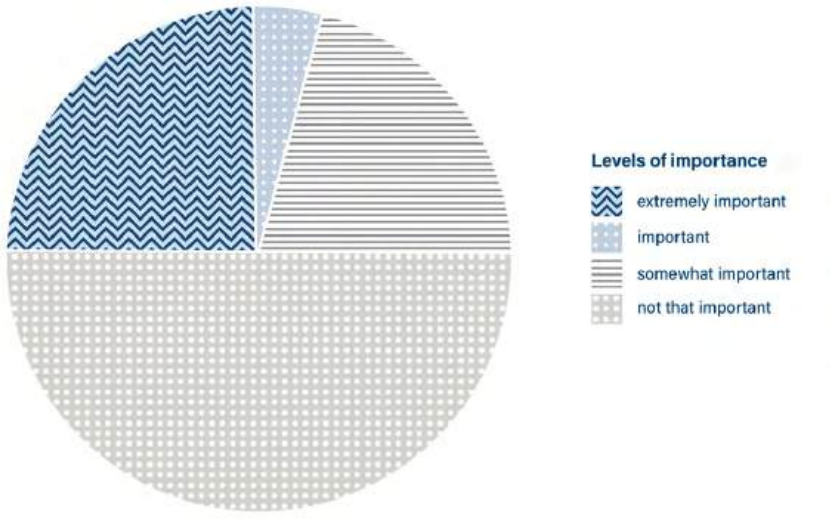


Figure 20: Relative emphasis of FVC cybersecurity standards.



Figure 21: Elements supporting the effective use of cybersecurity standards within the FVC.

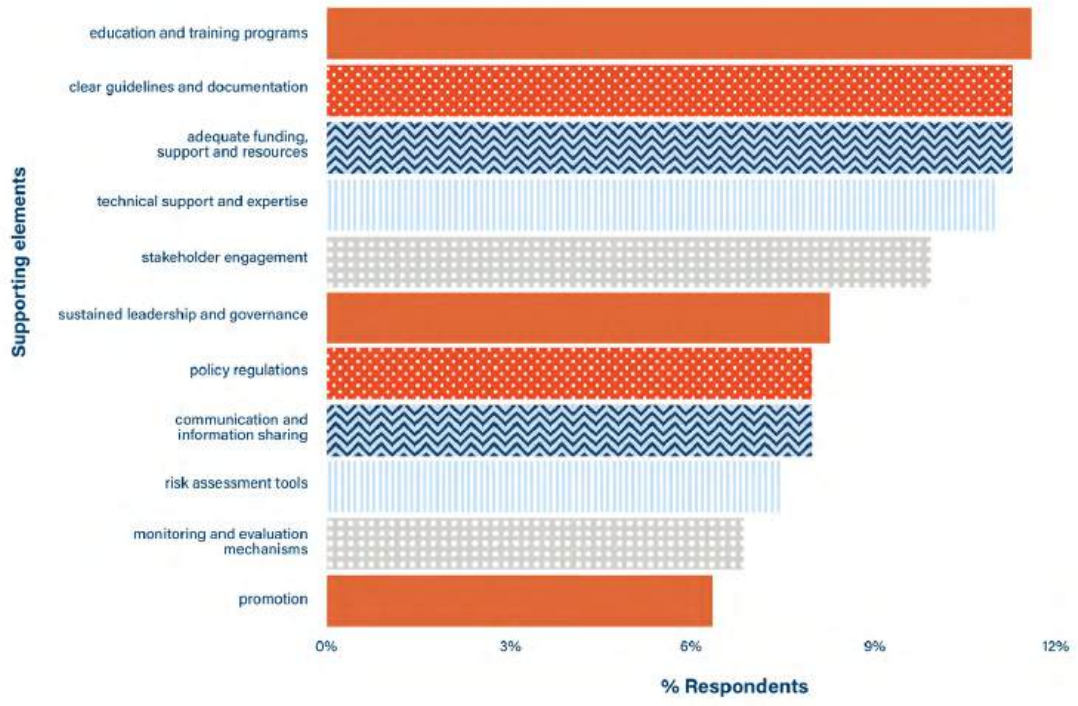


Figure 22: Options supporting enhanced cybersecurity capacity in the absence of sector-specific standards.

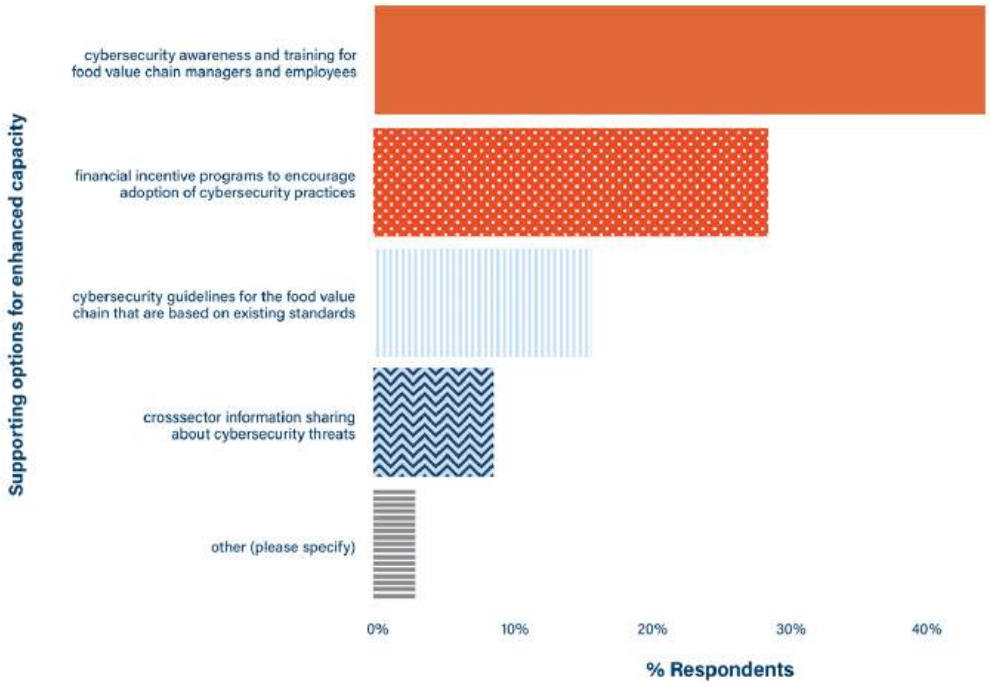
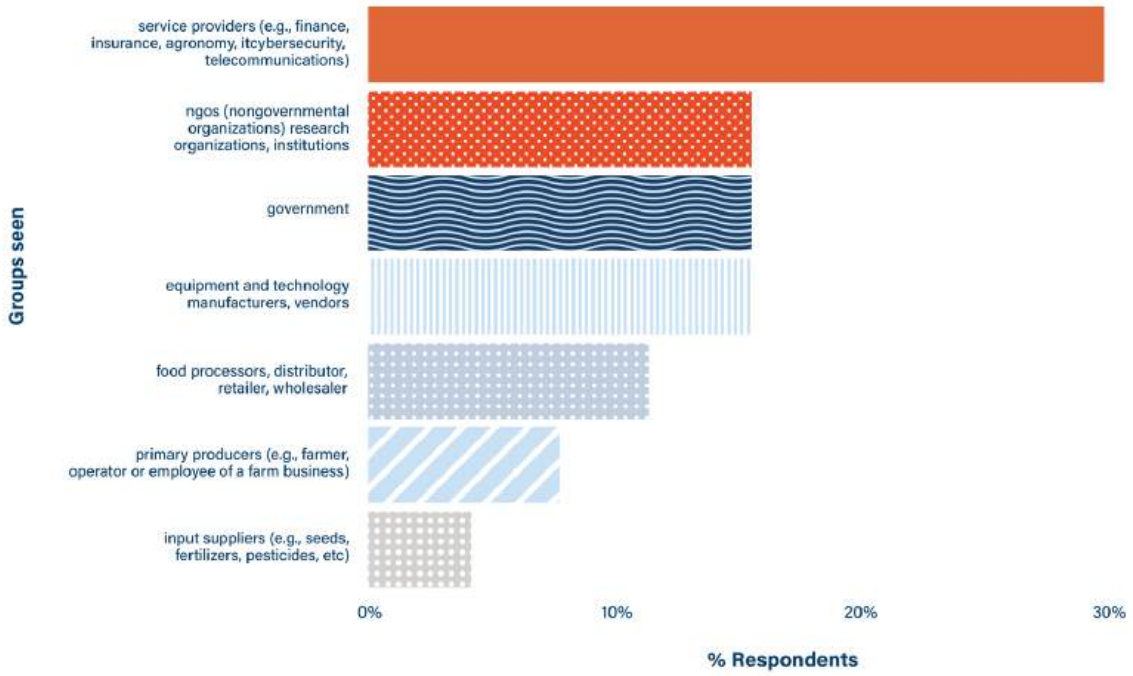


Figure 23: Groups seen as best positioned to lead cybersecurity capacity building in the FVC.



3.6.5.2 Who Should be Involved and How?

When asked to identify which groups should be involved in a cybersecurity standards initiative, respondents indicated that that they saw a role for a diversity of FVC actors: primary producers: 15%; food processors: 15%; service providers: 15%; equipment and technology manufacturers: 14%; government: 14%; input suppliers: 10%; NGOs or research institutions: 10%; other CIs: 8% (Figure 24). In addition to including those who are seen as being best positioned to support a cybersecurity standards initiative (cross-cutting organizations), respondents indicated that it was essential to include key supply chain actors, such as primary producers, processors, retailers, and so on. When asked about the most acceptable role for levels of government and regulators in a cybersecurity standards initiative, respondents generally identified support and the provision of funding through incentives programs (54%), as well as facilitating collaboration among relevant interested parties (25%), and creating and enforcing cybersecurity standards (17%). Four percent expressed that government should stay out of cybersecurity efforts entirely (Figure 25).

In their write-in comments, respondents suggested that cybersecurity must be recognized as a broad-based concern (not just within primary production and processing). Support was expressed for addressing cybersecurity in a comprehensive way. Respondents also suggested that competing priorities may overshadow investments to address cybersecurity risks, and that competition among relevant interested parties may make it difficult for common standards and infrastructure to emerge organically. One respondent worried that government-led initiatives could get bogged down in red tape, leading to difficulties in execution. Others emphasized that FVC actors need to see cybersecurity investments as a part of business, and as an important focus in a threatening and unstable world. Two participants identified having personal experiences with cyberattacks, one underscoring the need for greater awareness and preparedness. As one reflected: "We were preyed on through email and our financial institution. There are far more incidents than are acknowledged. People should be made aware of the risks and prevalence of cybercrime. It should be talked about." Respondent views on leadership and collaboration in developing cybersecurity standards for the FVC emphasized a strong role for industry-



led efforts, the need for inclusive engagement, and a supportive, not directive, role for government, though the latter view may be influenced by the sample's composition. Private industry, specifically service providers (including IT service providers) were identified as being best positioned to lead the development of cybersecurity standards. However, it was seen as essential to involve representatives from all key FVC actor groups in a collaborative, multi-sector process of standards development. Respondents suggested that the main function of government within a FVC cybersecurity standards initiative should be one of support, through the provision of funding and incentives for industry. However, it should be noted that this perspective might be skewed by the over-representation of primary producers in the survey sample.

3.7 Interviews with Food Value Chain Actors

3.7.1 Interview Participants

Twenty-one individuals from across the Canadian FVC were interviewed between March and May 2025. They spanned often overlapping roles that included inputs (e.g., fertilizers/nutrients), equipment (farm technologies), and services (e.g., agronomy, insurance, cybersecurity) (n = 5); primary production (n = 3); processing, production, and marketing (n = 6); distribution and retail (n = 3); technology and innovation/research (n = 4); and government/policy (n = 3). Consequently, participants were often able to speak from multiple perspectives.

Figure 24: FVC actors that should be involved in a cybersecurity standards development initiative (respondents could select as many groups of actors as they thought were essential to involve).

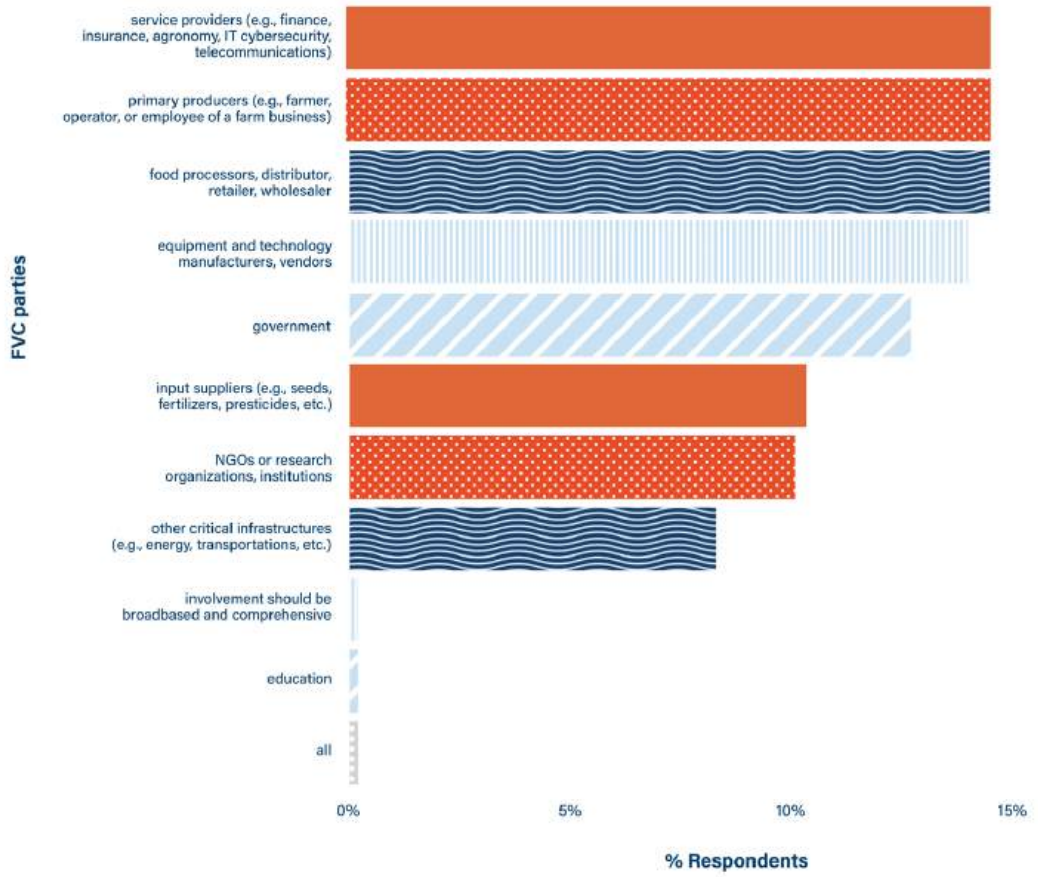
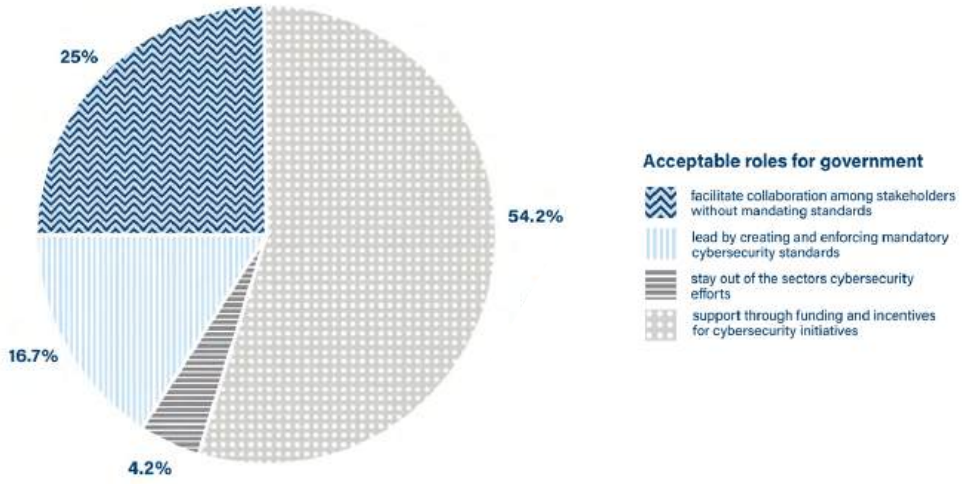


Figure 25: Respondent views on potential roles for government in a cybersecurity standards initiative.



3.7.2 Fragmented Readiness and Growing Digital Risk

Despite the expanding embrace of digital technologies across the FVC, participants saw cybersecurity readiness as uneven. Larger and more digitally sophisticated operations (distribution and retail enterprises, vertical farms) are adopting sophisticated technologies, such as enterprise resource planning systems, SCADA systems, and sensor networks, creating streamlined production and traceability. For example, among Canada's largest food retailers, one online retail and delivery business is known for the degree to which its core functions have been automated, from e-commerce to inventory management and the use of sophisticated robotic fulfillment systems. Similarly, large vertical farming businesses are fundamentally digital technology operations that are highly dependent on data analytics and automated control systems, and that also include critical connections involving input suppliers and output purchasers. In advanced vertical farms, traceability is enhanced through RFID tags and data logs that allow full visibility from seed to package. However, small- to mid-sized businesses, which includes many producers, continue to operate with legacy infrastructure, minimal cybersecurity awareness, and inconsistent practices. The third-party cybersecurity risk management requirements of large purchasers of vertical farm outputs often place stringent requirements on producers. This can mean that very small suppliers that lack cybersecurity capacity may have to be dealt with outside of an integrated input purchasing system. A growing reliance on digital infrastructure is evident even in routine farm management. As an agronomist observed: "It's not 'digital farming' anymore. It's just farming now. Everything is integrated—soil sensors, drones, field mapping—it's all digital." A dairy industry participant observed that some of the smallest provinces by size or population (such as PEI or Saskatchewan) are growing in their adoption of digital production technologies. Interviewees emphasized that businesses are also increasingly exposed due to their dependencies on digitized infrastructure, such as cloud-based traceability, e-commerce portals, and retailer-linked quality assurance systems. Despite this shift, older ways of doing things, such as the use of paper cheques and fax machines, remain prevalent in many agricultural operations—at least in many of those served by a major input supplier interviewed for this report. A participant from the agronomy and accounting arena noted that, in some cases, these practices (such as mailing or hand-delivering a paper cheque) are used by smaller businesses as an effort to make digital fraud less likely. Less secure practices, such as using messaging apps for financial communications or emailing access credentials to equipment or service providers, are still common. These represent significant vulnerabilities for electronic fraud, especially where business lines of credit may offer tempting targets for opportunistic financial theft. Even when the primary operations of a business are not digitally enabled, there may be elements of the organization's infrastructure that are potentially vulnerable to cybersecurity threats. Thus, one way or another, cybersecurity is an inescapable feature of all FVC components. Interviewees flagged the following key risks:

- Ransomware attacks, such as those that could affect livestock industries with narrow response margins (n = 2);
- Supply chain issues, including industry specific, siloed perspectives; a lack of attention and capacity related to cybersecurity; insufficient shared awareness and overall preparedness; potential data-based threats from foreign entities that could lead to disruptions; and uneven adoption of digital technologies, which would make standardization efforts more challenging (n = 15; 11 represented national perspectives, 2 were from Manitoba-based organizations, and one each from British Columbia and Alberta);
- Unsecured communication platforms and email compromise (n = 1);
- Multiple vulnerabilities, including those introduced via third-party vendors and equipment suppliers, and farm-based digital technologies (n = 21); and
- Trust issues, such as those involving digital agreements or poor visibility into data use (n = 9).

One participant, with perspectives spanning cybersecurity and food processing, distribution, and retail, suggested that some actors within supply managed sectors welcome forms of government



"Cybersecurity risks manifest differently across subsectors. In dairy and poultry operations, where robotic systems are commonly used, a cyberattack could halt operations and jeopardize animal welfare."

intervention that they view as beneficial but may be resistant to other interventions involving cybersecurity that they may view as intrusive. A vertical greenhouse executive, speaking to uneven levels of cybersecurity capacity among various input suppliers, suggested the value of developing some type of supply chain-spanning cybersecurity oversight. A government actor identified the importance of understanding supply chain vulnerabilities as a whole. Speaking to issues of trust and supply chain integrity, a participant from one of the agriculture federations echoed the value of strengthening third-party cybersecurity, such as among the suppliers of various inputs. Among producers, there is often a mindset of invulnerability. As a participant from the poultry industry observed, "It's still kind of a 'it won't happen to me' attitude." An emerging vulnerability facing Canada's FVC involves actions taken in the US that are widely viewed as degrading that country's cyber defence capabilities, including the dismissal of senior leaders in the National Security Agency and the US Cyber Command, as well as reductions in CISA's workforce [207]. Canadian CI protection has traditionally benefitted from information sharing and other joint initiatives with the US [208]. To the extent that the US becomes less able to identify looming cyber threats to its own national security, Canada may also be impacted, as some of these threats (such as those emanating from China, Russia, Iran, or North Korea) represent risks to this country as well [209].

3.7.3 Sector-Specific Vulnerabilities and Risks

Cybersecurity risks manifest differently across subsectors. In dairy and poultry operations, where robotic systems are commonly used, a cyberattack could halt operations and jeopardize animal welfare. According to one participant, "If a robotic milker goes down, that's a crisis." In such time-sensitive systems, downtime can result in overgrown livestock, missed production schedules, animal distress or death, as well as other significant losses. Processing plants are also at risk. With tight production schedules and just-in-time logistics, even a short disruption can ripple across the supply chain. In vertical farming, the threat landscape is highly complex. A participant from this sector observed that operations are entirely dependent on integrated control systems such as SCADA, enterprise resource planning, sensors, and data analytics that automate plant care, monitor environmental variables, and fulfill orders. Other vulnerabilities include the integrity of commodity sampling in international trade. As a participant representing field crop producers observed: "You ship something overseas and they sample it on arrival—how do you ensure integrity unless you digitize the sampling at the field level?" Without widespread implementation of security practices, data at rest or in transit can be manipulated to provide a false picture of a particular product. Interviewees reported the following distinct vulnerabilities by subsector:

- Primary agriculture: Weak password practices, shared logins, no backups; cyber risks heightened during planting/harvest cycles.
- Dairy and poultry: Data exposure via networked devices (e.g., photocopiers) and ransomware-linked shutdowns.
- Vertical farming and agtech: Highly digitized but exposed due to SCADA/programmable logic controller systems, limited air-gapping, and remote connectivity.
- Food processing: Strong dependencies on time-sensitive operations and international supply chains create high-value attack targets.

These vulnerabilities are exacerbated by factors such as limited cyber literacy, aging leadership, and lack of redundancy in rural infrastructure [5]. Human error is also a matter of consideration in cybersecurity planning. As a vertical farm executive reflected: "The idea is to take humans out of the equation—to the extent possible." From fraud attempts via email spoofing to supply chain miscommunication, vulnerabilities are expanding with the digitization of every link in the FVC. Some vulnerabilities are deeply embedded in informal communication practices, such as the use of messaging apps for financial transactions and communications. Email fraud and bank transfer scams are not uncommon. As one food and beverage industry representative shared: "Some of our members were victims of ransomware."

3.7.4 Potential Role for Cybersecurity Standardization

There appears to be tentative conceptual support for cybersecurity standardization, keyed to the unique features of the Canadian FVC value chain. Several potential benefits were identified, including:

- Protective benefits:
  - Establishing a consistent and baseline level of cybersecurity across the FVC;
  - Serving as a common framework for driving improvements in cyber hygiene practices;
  - Providing a basis for validating and improving organizational security practices; and
  - Identifying sources of threats.
- Practical benefits:
  - Increasing trust in monitoring and traceability systems;
  - Establishing clear guidelines for technology development (security-by-design) and adoption;
  - Identifying contamination/spoilage;
  - Revealing data integrity issues (e.g., data breaches, data poisoning);
  - Enhancing operational lines of sight to better manage bottom-line; and
  - Supporting systematic approaches to risk identification and mitigation.
- Strategic benefits:
  - Supporting FVC performance and resilience;
  - Aligning with global trade requirements (e.g., EU, US);
  - Providing competitive advantage for compliant organizations;
  - Clarifying roles and responsibilities across the value chain; and
  - Facilitating better communication and trust between different value chain participants.

However, interviewees consistently stressed that standards must be practical, flexible, easy-to-understand, and scaled to reflect:

- The diversity of actors (from one-person farms to national processors);
- Different levels of digital maturity across FVC businesses;
- Sectoral and regional contexts (e.g., organic farms vs. vertical farms; livestock vs. field crops); and
- The operational cadence of farming cycles and just-in-time logistics.

Participants from the retail, commodity, and agronomy sectors cautioned against rigid, top-down approaches. Instead, they called for modular, maturity-based standards that recognize the diversity of operators and their differing digital capabilities. Several recommended a tiered or maturity-based approach, featuring low-barrier entry points (e.g., email security, backups) and advancing toward more rigorous standards as readiness improves. Support for this pathway of learning and practice change might benefit from being positioned as

not unlike other everyday practices and requirements of FVC parties. For example, participants from commodity (n = 2), agricultural policy (n = 1), government (n = 2), equipment and input supplier (n = 1), and agronomy (n = 1) perspectives identified strong parallels with food safety standards. As a consultant to the agricultural industry noted: "Farmers already deal with global food safety standards. Cybersecurity should be framed the same way." Participants referenced GS1 traceability (a set of global standards to enable end-to-end traceability of products as they move through supply chains) (n = 1) and HACCP protocols (n = 7) as helpful models.

3.7.5 Enablers and Strategic Levers

On the theme of a learning and practice change journey, awareness building was viewed broadly as the most important step towards enhanced cybersecurity (n = 15, spanning retail, technology innovation, commodities, policy, government, insurance, and agronomy perspectives). Education and training on cybersecurity, and access to relevant, practical resources, were viewed as helping to set the stage for an improved cybersecurity posture. Incentives, particularly for SMEs, were also mentioned as potential opportunities to underline the value of adopting effective cybersecurity practices, while mitigating barriers related to limited resources and smaller profit margins. A technology executive suggested that storytelling and real-world breach narratives can be important catalysts for awareness and engagement. Real-world breach stories were experienced as powerful motivators, as demonstrated by food sector organizations that have used social engineering case studies to boost training participation. To drive improvement, interviewees emphasized the importance of trust, partnerships or working through trusted channels (n = 8, from the cooperative, technology, dairy, processing, insurance, input, and government perspectives). Businesses that embody and demonstrate trust and farmer-focused cooperatives and industry associations were provided as examples of trusted partners. Some also added equipment vendors to this list. One interviewee, with extensive experience consulting across the food system, commented: "Start with the dealers—they're trusted." To avoid overwhelming producers and other small and medium business owners with yet another program, cybersecurity training could be integrated into existing programming, such as those addressing occupational safety and mental health. Embedding cybersecurity into existing food safety and animal welfare frameworks is another recommended strategy for reducing the perceived administrative burden of cybersecurity training and practice change.

Technology solutions that build resilience, such as battery backups, segmented networks, and traceable digital records, were highlighted as potentially appealing avenues for introducing discussions and options for enhancing business cybersecurity. Among producers, agronomists and insurance providers, as well as information communication and telecommunications providers may play critical roles in supporting practice changes in cybersecurity as partners and essential components of business risk management, respectively. For example, financial institutions and insurers might use standards as a basis for determining the eligibility of agri-food businesses for various financing or insurance package pricings. As one food processor and cybersecurity expert pointed out, financial institutions could be in a helpful position to link businesses to insurance options. However, as an agronomist noted, financial institutions might not be seen in a positive light by some in the producer community. A government official suggested "fram[ing] cybersecurity as a [manageable] journey, starting with backups and email hygiene."

The insurance industry was acknowledged by a number of interviewees as having a potentially useful role to play (n = 7, spanning commodity, policy, and insurance sectors, and government). Insurers were identified as being positioned to drive cybersecurity improvements across the FVC because they could reduce financial impacts from cyber incidents that could shut down FVC businesses. Standards and guidelines are seen as ways to demonstrate due diligence, create a common language for basic cyber hygiene, and provide a roadmap for capacity building that insurers can align to. Highly automated equipment and smartphone-centred operations may, paradoxically, lead to more downtime and loss severity if used as entry points for cyberattacks. Interviewees emphasized

that policy conditions with teeth (e.g., required phishing tests tied to coverage) can help shape positive cybersecurity practices. They also noted potential risks involving situations where business data could be used against policy holders by the insurance industry.

A digital equipment manufacturer suggested that some of these cross-cutting service providers (e.g. smaller advisory firms) may be less up-to-date on contemporary cybersecurity issues and practices. Developing cybersecurity awareness and best practices among these groups could be an effective way both to mitigate a less visible vulnerability within the FVC and to spread awareness and practice knowledge to their agricultural clients.

In addition to serving as a reference point for government-funded incentive programs for cybersecurity practice enhancements, a cybersecurity standards initiative could form the basis for public–private partnerships enabling accessible grant programs along with auditing and other shared services that are essential to effective implementation. Funded pilots, awareness campaigns, and certification incentives were identified as collaborative opportunities to accelerate progress towards enhanced cybersecurity readiness. Also suggested was the need for safe, anonymized breach reporting mechanisms to foster a culture of learning without fear of financial repercussions or reputational harm. From the standpoints of consumer safety and trust, the operational implications of this suggestion would require a careful work-up.

Finally, a multi-party approach is essential for promoting technology adoption by addressing ethical and cybersecurity issues [210] through dialogue and shared learning. For example, a variety of teleoperated robotic systems are emerging [211] that offer the promise of operational efficiencies across all aspects of the FVC. Some of these business efficiencies may entail both positive and negative social impacts. These systems may also contribute to sustainable development goals within primary production, such as preserving biodiversity, as elements of precision agricultural operations [210]. However, as a digital equipment manufacturer observed, robotic systems that are operated by third-party teams of humans may be exposed to new types of physical and cybersecurity security risks, including the weaponization of mobile platforms. Emerging issues of this kind can be best identified and addressed through processes that involve a diversity of perspectives working in collaboration. Recognizing the complex challenges associated with developing and implementing suitable cyber insurance products, an insurance industry executive suggested the value of holding cross-sector forums to enable a better understanding of the risk environment and risk management opportunities.

3.7.6 Governance and Leadership

In various ways, participants suggested that food system cybersecurity would be best achieved through collaboration or partnership. For example, participants from government and the insurance and agronomy sectors (n = 3) identified that there are roles for a variety of actors. A government participant suggested that, while government should be a partner in building better cybersecurity capacity, the process should be led by industry. Larger actors were seen as being key to creating the conditions for successful standards development and adoption, and a corresponding shift in business practices. Existing organizations, such as those focused on traceability, breed and genetics associations, and certain cooperatives, already steward large volumes of data, and could therefore be pivotal in leading change. Similarly, through their third-party cybersecurity risk management programs, large retailers can help to create a "pull" effect—bringing those who provide inputs to their business processes into alignment with new requirements. A coordinating structure that includes private sector innovators, universities/research groups, standards bodies, and regulators is widely seen as both practical and necessary. Interviewees voiced interest in the idea of a multi-party governance model, with government playing a supportive or co-facilitative role (e.g., funding, convening) rather than leading such a group outright.

3.8 Key Gaps and Challenges

A prevailing sentiment among agri-food business owners is one of administrative overload from current safety and compliance programs. Many FVC enterprises operate with slim margins and limited available capital. Even within profitable enterprises, this appears to be a

widespread concern. This could constrain the sense of priority, the motivation, and the capacity of business owners to invest time and capital in cybersecurity, or to embrace the benefits of a voluntary standardization initiative. Adding a cybersecurity program on top of the other demands on their attention and resources may exacerbate administrative fatigue, especially among smaller businesses. A participant and cybersecurity expert from the poultry industry reflected: "They think, 'we're small, so why would they target us?" Building cyber preparedness is like investing in broad health promotion initiatives. The benefits may not be immediately evident to the average person or business. Moreover, interest in adopting cybersecurity standards may be hampered by a perceived lack of return on investment at the business level. Some of this hesitancy may stem from insufficient integration with existing food safety, quality, and sustainability systems, with a corresponding lack of visibility on interdependent vulnerabilities. This challenge was described by a FVC infrastructure provider: "Even organizations like [some of] the large grocers and the large food service distributors don't necessarily have a digitized supply chain, and so that for them to truly leverage standards, there has to be an ROI on it, and it's hard to get at that ROI. Even Canada is behind a lot of places in the world and in our ability to trace our food. . . because we didn't invest in digitizing our supply chain to make it really easy to track where problems may be or where problems could be coming. . . people don't know that they don't have line of sight because. . . their systems aren't set up to do such a thing."

It was also revealed that there is an element of vendor mistrust among some agricultural producers (not unrelated to the right-to-repair movement and data ownership and privacy concerns). This may contribute to an aversion toward fear-based messaging about cybersecurity risks. This contrasts with other findings suggesting that vendors are also seen as trusted sources of information about the products they sell. There is no one-size-fits-all approach to communication and outreach. Consequently, it will be important to work collaboratively to identify the most trusted channels for information and engagement within particular subsectors and regions of the Canadian FVC. At the time of writing, formal and systematic



attention to cybersecurity across the FVC is limited. There is a gap in leadership and coordination involving both government and industry that represents an important opportunity for impact. As one respondent from the food manufacturing sector suggested: "[o] nly when private equity enters [the scene] do firms get the tools to modernize." A participant also suggested that cybersecurity remains underprioritized within the food manufacturing industry due to the sector's low political visibility compared to primary agriculture, despite its critical role in national food security. Others saw large retailers as potentially important drivers of practice change among primary producers and food manufacturers. Two areas offer promise here: consumer and trade expectations around food traceability, and third-party cybersecurity risk management. Some interviewees felt that the needs of large purchasers for secure system-to-system communication and reliable product data may create an important pull effect, driving others to improve the cybersecurity practices that underlie these transactional requirements. While the business case for cybersecurity appears widespread across larger entities within the FVC, it was seen as being far less pronounced as a regular part of business risk management among smaller actors. Importantly, there appears to be a general lack of attention to the broader systemic risks of low attention to cybersecurity across the entire FVC.

Poor digital practices compound the problem. Shared logins, unencrypted communications, and reliance on free or consumer-grade apps for business purposes are common. "People get overwhelmed by the jargon and fear-based marketing," explained a cybersecurity expert with a large retailer. Additionally, many organizations are simply unaware of best practices or unmotivated to prioritize them. Reflecting the findings of earlier research in the agricultural sector [5], the prevailing mindset on cybersecurity among many smaller FVC businesses appears to be one of security through obscurity. Although existing cybersecurity standards offer many benefits that can be leveraged to secure information systems and industrial control systems, they exhibit limitations beyond those identified in Table 11 when applied to the unique environment of today's FVC. The pace and mechanisms for considering new threat intelligence and updating standards may no longer be fit-for-purpose in an environment of accelerating technological change. In addition, a number of notable challenges exist related to the implementation of any cybersecurity standards across the breadth of the FVC. While many other CIs benefit from guidance on cybersecurity, the food system lacks a coordinated perspective, along with sector-specific guidance for individual components. There is a lack of tailored recommendations that address the unique environmental and operational challenges of the various operational settings within this environment. Yet, as digital transformation through IoT, AI, and automated systems becomes more prevalent, the food system will face new, and more numerous, cybersecurity risks.

Current standards and frameworks often focus on information security management systems applicable to any organization but do not address the unique challenges of the FVC. There is a scarcity of guidelines that consider the specific operational technologies used in food production and processing, leading organizations to adapt generic standards without tailored guidance, potentially resulting in inconsistent implementation and security gaps. With a global rise in supply chain attacks, one of the most significant gaps relates to the improvement of supply chain security. This includes third-party vendors and the integrity of physical inputs. Agricultural operations and food processors depend on a complex, global supply chain involving equipment manufacturers, software developers, input producers, and service providers. Cyberattacks targeting any point in this chain can disrupt the entire food production process through cascading impacts. These supply chains introduce vulnerabilities that are not fully addressed by existing standards. Although ransomware operations may target supply chain pinch-points to intensify the pressure to pay, the more significant risk for widespread harm comes from ideologically or geopolitically motivated actors. In the first case, this could involve foreign or domestic actors seeking to disrupt CIs consistent with a particular cause. In the second case, this may involve using cyber tools as hybrid elements of foreign interference or, more seriously, as part of asymmetrical operations that also involve physical combat. The diversity of malicious actors (criminal, ideological, or geopolitical) and the range of exploits they can deploy, call for attention to mechanisms within the FVC for continuous monitoring, proactive threat detection, and reporting, along with producing and disseminating cyber threat intelligence. These would boost the situational awareness of individual businesses as well as support systemic collaboration. Protocols for intelligence sharing, such as setting up sector-specific ISACs would also deepen the capacity of the FVC to make data-informed decisions closer to the "speed of cyber." These kinds of proactive approaches may not only prevent cyberattacks from causing major operational disruptions but may also allow for faster recovery in the case of an incident, supporting long-term resilience.

The FVC, with a power balance emphasizing the needs and interests of larger businesses [1], often lacks transparency regarding vendors' security practices. Farmers and smaller processors may have limited visibility into the cybersecurity measures implemented by their suppliers and service providers, making it difficult to assess and mitigate risks associated with equipment, devices, or other third-party components. Cybersecurity standards currently do not provide sufficient guidance for FVC end-users on how to evaluate cyber risks. Data governance, ownership, and privacy protection present additional challenges in the agri-food sector, and therefore the FVC, that are not addressed directly by existing standards and frameworks. Farmers are often clear they believe they own the personal and business data originating

within their operations, but they remain uncertain how technology vendors implement data access and control measures and how their farm data is used beyond their operations. From a data governance perspective, there is a need for broader and deeper consideration of data ownership complexities and privacy concerns specific to FVC system data.

Industry-spanning dialogue on ways to optimize cybersecurity response capacity while minimizing exposure to legal liability where an operation includes a mix of proprietary data streams could address a particularly important barrier faced by some farming operations: a vendor may be reluctant to investigate certain on-farm data issues if there is a risk that they could inadvertently view another vendor's proprietary data, as this could place the first vendor in jeopardy of civil litigation.

The implementation of cybersecurity standards also has major implications for the protection of OT used in the FVC. Food production and processing systems, including automated machinery and IoT devices, are often vulnerable to attacks, particularly when legacy systems that were not designed with cybersecurity in mind are involved. IEC 62443, which is tailored for industrial control systems, offers an example of how organizations can secure both new and legacy OT environments. This lowers the risk of disruptions to critical production processes, ensuring the continued safety and quality of food products.

The integration of legacy equipment with modern smart technologies also poses security challenges that are not fully covered by existing standards. Farms and smaller processing and retailer operations that use older machinery lacking built-in security features could experience vulnerabilities when these machines are connected to networks. Current standards do not provide detailed guidance on securing such hybrid systems, leaving a gap in effectively protecting environments where legacy equipment interfaces with new technology. While legacy equipment poses a major risk, upgrading it, or safely integrating legacy components into new structures, may be cost-prohibitive. Along with a sense of complacency, this is detrimental to achieving an improved cybersecurity posture. Some of the ways that this issue might begin to be addressed include:

- Incremental security enhancements: Making practical, lower-cost options available, such as installing firewalls, network segmentation, or encryption tools that are compatible with older systems.
- Transition incentives: Government or industry grants could be provided to help FVC entities gradually transition to more secure, up-to-date systems.

Regulatory gaps, consumer trust, and compliance burden also present significant challenges. In Canada, there is no comprehensive cybersecurity regulation specifically focused on the agri-food industry [124], as has started to emerge for other CIs (such as federally regulated entities, per recent Canadian legislation). Without a degree of regulation and accompanying standards, cybersecurity measures vary widely among organizations, and weak links in the value chain can compromise the entire network. As data protection regulations such as the GDPR become more stringent, compliance with cybersecurity standards could help organizations avoid legal penalties and demonstrate their commitment to securing both data and operations. Some alignment with internationally recognized standards could enhance consumer trust and build stronger relationships with relevant interested parties by ensuring that the FVC is protected from cyber threats. However, meeting cybersecurity regulatory requirements can be particularly challenging for SMEs within the FVC, which may lack the administrative support or the capacity to navigate complex compliance obligations. This challenge might be surmounted in two ways.

- Development of simplified compliance tools: Create simplified, scalable compliance frameworks tailored to the needs and capacities of FVC.
- Introduction of a sector-specific framework: Consider sector-specific guidelines that prioritize essential practices for the FVC, making it easier to comply without the burden of larger, more complex, generalized cybersecurity frameworks.

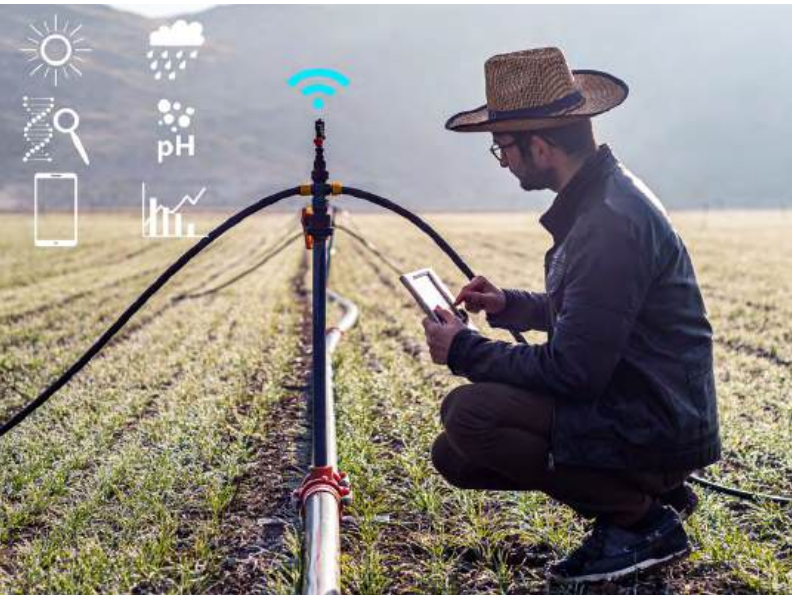
There is limited integration of cybersecurity with food safety management. Food safety standards like HACCP and ISO 22000 do not typically incorporate cybersecurity considerations [33]. Cybersecurity and food safety are often managed independently, leading

to gaps where cyber threats that affect food safety may not be adequately detected or mitigated, posing risks to consumer health.

The resource constraints faced by SMEs considering the adoption of cybersecurity standards are consequential for widespread implementation. Comprehensive cybersecurity frameworks such as ISO/IEC 27001 and IEC 62443 can be resource intensive, requiring not only financial investment but also personnel with the skills to ensure that the associated activities take place. Adopting prioritized cybersecurity controls would help smaller organizations achieve a basic level of cybersecurity without overwhelming financial burdens. To be effective, any standards-based solution must be developed by those who understand the cybersecurity landscape of the operations needing protection, including the safeguarding of information assets and networks, and the broader threat environment within the business context. Where implementation is concerned, smaller businesses in the agri-food sector often face awareness and technical knowledge gaps related to cybersecurity. Partial or inadequate implementation leaves organizations vulnerable, making it essential to develop scalable and adaptable frameworks that fit the varied needs of different organizations in the agri-food sector. In some settings within the FVC, such as primary agricultural production, where digitalization is relatively new, there is resistance to adopting cybersecurity practices, especially as they are seen as costly or complex. Actions that could help address this challenge include:

- Awareness campaigns on cyber risks in specific areas of the FVC: Industry associations and cooperatives can lead campaigns to raise awareness about the sector-specific risks and impacts of cyber incidents, shifting the perception of cybersecurity from a "tech issue" to a business priority.
- Education and training initiatives: Industry bodies and government agencies can offer training workshops, online courses, and certification programs specifically designed to raise cybersecurity awareness and skills within the FVC, including awareness workshops for rural residents, accessible training for small business owners and growers [e.g., 177], role-specific cybersecurity training for farm managers and owners of small food processing operations, and technical training for designated personnel across the FVC. Additional specialized training opportunities that focus on the unique needs of other components of the FVC will also be needed. Cybersecurity literacy within the FVC can be developed through partnerships between industry and educational institutions. Just as food system actors should have a baseline knowledge of cybersecurity, those entering careers in cybersecurity should understand the unique needs of the FVC and the rewarding opportunities that may come from building a career serving the needs of this sector [11].
- Development of clear, user-friendly guidelines: Providing simplified, actionable guidelines on core cybersecurity practices can make it easier for non-technical parties to adopt security measures. Guidance, provided by trusted channels, to help businesses secure hybrid environments where legacy equipment interfaces with modern technology would be beneficial.

There is a gap in addressing the cyber-physical security aspects unique to the FVC. Cyberattacks on digital agricultural systems can have direct physical consequences across the FVC, such as manipulating irrigation systems or altering climate control parameters in primary production, disrupting tracking and logistics in distribution operations, or interfering with robotic fulfillment processes in retail businesses. Existing cybersecurity standards primarily focus on information security and may not comprehensively cover the prevention and response to attacks that span both cyber and physical domains. Standardized protocols and security measures specifically designed for IoT devices used in the FVC are also lacking. The diversity of devices used in digital agriculture creates a heterogeneous environment that is challenging to secure with generic standards. Existing IoT security guidelines offer general recommendations but may not address the operational conditions and threats specific to agriculture, such as the need for devices to function reliably in harsh weather conditions and isolated locations with limited connectivity. The evolving cyber threat landscape, including the use of AI-driven cyberattacks and advanced hacking techniques, requires that standards solutions remain flexible and adaptable. Implementing cybersecurity frameworks is



"Climate-related disruptions, such as extreme weather events, are not currently addressed in standards frameworks but could have significant implications for cybersecurity, particularly in rural and remote areas."

not a one-time effort; it involves continuous updates to address new risks. Standards and guidelines must evolve alongside technology to cover emerging threats, such as AI-driven attacks that target the automation in food production systems or blockchain vulnerabilities in supply chain management. Flexibility can help organizations stay ahead of the ever-changing cyber threats facing the sector. It also is important to understand that, just as AI can be weaponized by malicious actors, it can also be deployed as a shield against their exploits. Additionally, there are sustainability and environmental implications tied to cybersecurity standards implementation. As sustainability practices become increasingly integrated into food production, the need to protect environmental data, such as water usage, pesticide levels, and soil health, becomes more critical. Cybersecurity standards could support the integrity of this data, which is essential for sustainability reporting and regulatory compliance. For example, protecting data from tampering ensures that accurate environmental metrics are maintained, helping organizations meet sustainability goals while also safeguarding their reputations.

Climate-related risks on digital infrastructure must also be assessed and considered in formulating FVC standards. Climate-related disruptions, such as extreme weather events, are not currently addressed in standards frameworks but could have significant implications for cybersecurity, particularly in rural and remote areas. Increasingly frequent climatic events (e.g., floods, fires) can affect IT infrastructure and security systems across the FVC. Features related to fostering climate resilient systems should be considered and built into cybersecurity practices. These might include securing backup power, developing climate-related disaster recovery plans, and ensuring that remote operations are resilient against physical disruptions. The need for cyber insurance and enhanced risk management practices within the agri-food sector is becoming increasingly important. At the same time, cyber insurance is a developing space. As noted by an insurance industry executive, while more and more components of agri-food operations have a cyber nexus, cyber insurance is currently not considered a profitable cost centre within the insurance industry. There is important work to be done to refine a business model, and underwriting practices that will enable a clearer and more sustainable role for cyber insurance as a critical tool for agri-food business risk management, aligned to FVC operational environments and risks. As this continues to develop, attention to cyber risk assessment and proactive cybersecurity practices will be important, as they are often prerequisites for obtaining, and maintaining, favourable coverage at a manageable cost. Standards could be an important focus for getting this right. Finally, the Canadian FVC currently lacks a unified, coordinated, all-of-system focus. Standards development and implementation could therefore be grounded in collaborative processes that consider the interconnections between the FVC and society as a whole, which involve multiple parties and draw from an interdisciplinary perspective.

Collaborative processes, incorporating a diversity of technical, operational, and social perspectives (including those of women and Indigenous business owners), will help to identify how standards, and which adaptations, would best lend themselves to the needs of the sector. For example, in the arena of food security, there is a growing understanding that historical colonial practices and policies have harmed Indigenous food sovereignty, both directly and indirectly, through their impacts on Indigenous women and, by extension, their communities [212]. Consequently, bringing the voices of Indigenous peoples and women into discussions of how the Canadian FVC functions may be seen as an element of reconciliation [213]. Incorporating a diversity of viewpoints and lived experiences on FVC cybersecurity can also help to ground emerging solutions within a broader set of insights. More broadly, the lack of attention to FVC cybersecurity in the academic, policy, and standards literature calls for an expansion of focus, which could be achieved by convening and integrating perspectives from across this CI. Implementing cybersecurity standardization in the FVC extends beyond mere risk mitigation. Standardization can help provide a foundation for securing supply chains, preserving data privacy, ensuring operational continuity, futureproofing against emerging threats, and strengthening the social contract among relevant interested parties. Addressing the gaps and challenges discussed in this section will require developing specialized frameworks and guidelines that consider the distinctive characteristics and needs of the broader agri-food sector. Such efforts will ensure that cybersecurity measures are both effective and practical for farmers and agri-food related businesses, ultimately safeguarding the integrity and resilience of our food system.

4 Conclusions and Recommendations

4.1 Conclusions

FVC integrity is more than a digital concern; it contributes to the economic resilience, prosperity, stability, and cohesiveness of Canadian society. The cybersecurity of the FVC is an issue of national security [8] because it touches on food security, individual and population health, regional and national economic prosperity, social and societal wellbeing and resilience, and geopolitical position. Food is increasingly being weaponized as focus of hybrid operations by a variety of foreign actors, including adversaries in international trade and geopolitics. Cascading failures are possible if core digital infrastructures are compromised. As one interview participant from a provincial federation observed, "If you encrypt our. . . systems, millions in exports stop. We can't market, can't decide—everything halts." Canada lags behind other jurisdictions that have undertaken work to develop integrated frameworks for addressing multi-level cybersecurity challenges, particularly in the agri-food sector. For example, the US Food and Agriculture ISAC [125] seeks to address the unique challenges faced by the agri-food industry, the EU's NIS2 Directive addresses ways that the food system can integrate cybersecurity practices with regulatory requirements to protect CI, and the Netherlands Cybersecurity Strategy illustrates the potential value of a holistic, all-of-society approach to cybersecurity. Furthermore, a set of potential cyberattack scenarios developed by the US Department of Homeland Security has proved to be both farsighted and useful as a focus for much-needed attention [107]. Recent peer-reviewed research underscores the importance of efforts involving public–private collaboration on standards to benefit the cybersecurity of CIs [214], and specific components of the FVC [12]. In Canada, a report from the House of Commons Standing Committee on Public Accounts concluded that Canada's food system lacks coordinated resilience planning and urged greater attention to emergency coordination and long-term resilience through enhanced data, workforce development, and collaboration across sectors [215]. To enhance cybersecurity across the FVC, a cybersecurity framework that is tailored to the unique vulnerabilities and operational needs within this sector could play an essential role. Strengthening collaboration, such as through public–private partnerships, is crucial for effective information sharing and resource distribution, enabling coordinated responses to cyber threats and improving resilience [11]. Comprehensive education and training programs should be implemented to elevate cybersecurity awareness and skills at all levels of the FVC, from farm operators to retail managers [11]. Furthermore, standardized incident response and

recovery protocols must be established to ensure swift and effective actions during cyber incidents. A practical reporting scheme would also elevate insights and inform coordinated planning and policy development. Lastly, providing incentives for early adoption [11] and demonstrating the benefits through pilot projects could facilitate widespread uptake of these technologies. Implementing robust cybersecurity measures within the FVC presents several challenges due to its complexity and the diversity of its interconnected components [13]. Tailoring solutions to meet specific needs from production to retail is an elaborate task. Smaller enterprises often face significant resource constraints, lacking the financial and technical capabilities necessary to implement sophisticated cybersecurity measures. The rapid evolution of the cyber threat landscape requires constant vigilance to keep security measures updated and effective against new threats [216]. Regulatory and compliance issues also pose a challenge, as relevant interested parties must navigate a complex landscape of data protection laws while participating in an innovation ecosystem. Finally, engaging a broad spectrum of relevant parties, who possess varying levels of knowledge and interest in cybersecurity, is critical. Overcoming skepticism and aligning collective efforts toward robust cybersecurity investments is essential for safeguarding the entire FVC. Together, these challenges underscore the importance of the human element in the people, processes, and technology flow. While it is technology and processes that are often foregrounded in discussions of cybersecurity and cybersecurity standards, attending to the people challenge is a prerequisite for the other two elements to succeed. This is especially true in the face of such complex, systemic, problems as FVC cybersecurity, which no single party can address on its own. These benefit from collective efforts involving coordinated collaboration across multiple sectors, built around common goals [217]. There is a growing understanding that cybersecurity in the FVC needs to have a dual focus on:

- Threats and impacts disrupting individual businesses; and
- Threats and impacts affecting the broader system and the public.

Cybersecurity standards or guidelines have a critical role to play in both arenas. At the time of writing, there are no cybersecurity standards, guidelines, or compliance regimes specific to the FVC, or that recognize the value of a dual focus on individual components and systemic integrity.

On a day-to-day basis, small and large business owners are seized with a variety pressing concerns that often push cybersecurity into the background, when it is considered at all. This needs to change, but attention to cybersecurity should not compete with more readily understood strategic enterprise issues, or with the attention and resources available to business owners and operators. Credible industry champions and narratives that explain the practical business case for cybersecurity were identified as important ingredients of practice change. Cybersecurity should also be embedded in the practices and processes of cross-cutting organizations, such as service providers, as well as being a design feature and marketing strength of equipment manufacturers. Where possible, cybersecurity should be incorporated into already-accepted programs, such as those having to do with occupational health and safety, or compliance regimes that depend on the confidentiality, integrity, and availability of critical data, such as the HACCP framework for food safety.

The FVC is a large, complex, and highly variable system of systems, processes, and actors. As a result, it may be most effective to consider a modular approach to enhancing cybersecurity through standards or guidelines anchored to cyber maturity levels. One move in this direction is the CCCS's Baseline Cyber Security Controls for Small and Medium Businesses [137], which have been described as "the Canadian specification of controls equivalent to that of the NIST Cyber Security Framework [5] or ISO/IEC 27001" [132]. Another is IEC TS 62443-1-5, which provides implementation guidance for CI [193]. While the implementation of a Canada-specific cybersecurity framework for the FVC means different things to different actors, what is clear is the need for a suite of resources that balance multiple considerations, including Canadian food sovereignty, international trade opportunities and requirements, regional and sectoral differences, and the benefits of multi-sectoral collaboration. At the same time, it will be important to recognize that international standards can facilitate trade diversification. Thus, any standardization initiative must strike an effective balance between the needs and interests of Canadian FVC actors and their

trading partners abroad. The most important findings may be those having to do with the human, relational dimension of cybersecurity, specifically the need for sector engagement, outreach, and most importantly, awareness building and guidance, leveraging trusted channels. Drawing from concepts in data and cybersecurity governance, a type of federated governance model may lend itself to the developmental needs of the FVC related to CI cybersecurity. Federated governance involves a collaborative structure where multiple independent organizations or actors share responsibility for decision-making, implementation, and oversight, typically within a complex system or sector. Instead of a central authority exercising full decision-making authority, a federated model distributes leadership and roles across trusted organizations that work together under common goals or standards. For example, a recent examination of federated data governance models [218] observed that this type of structure is more adaptable in the face of such common challenges as:

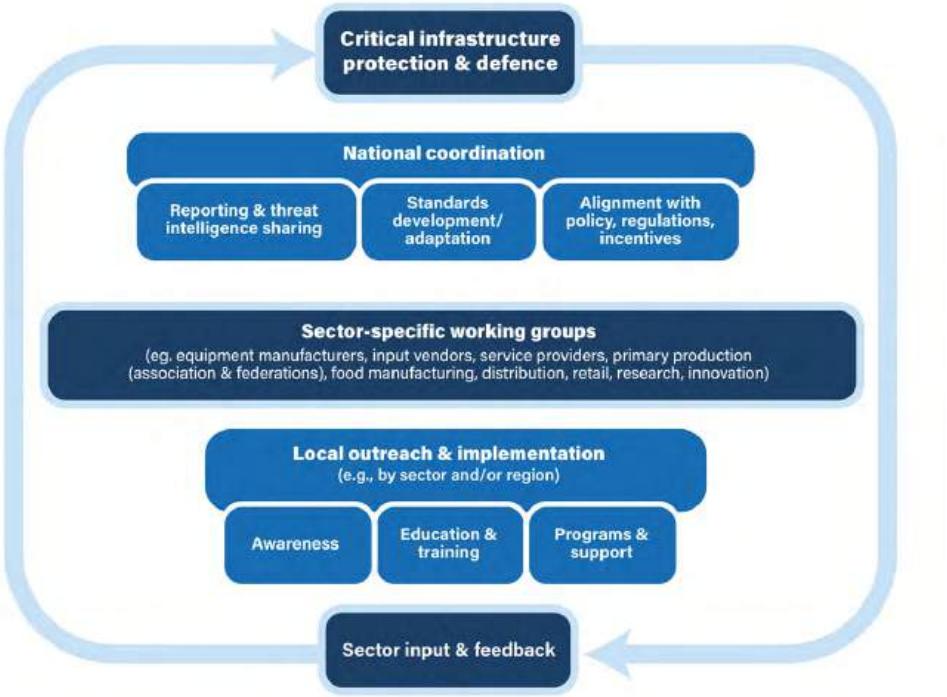
- Blind spots related to a diversity of regulatory compliance regimes;
- Coping with mixes of modern and legacy data systems;
- Adjusting to new business needs or advances in technology; and
- Change management issues.

As shown in Figure 26, while CI cybersecurity is more complex than organizational data governance, the core features and benefits of a federated model can serve as a useful reference point, or at least a conceptual starting point, for evaluating potential structures tailored to the FVC.

A decentralized, collaborative model for developing and implementing cybersecurity standards in the FVC recognizes that no single authority can effectively manage cybersecurity across such a complex and decentralized system. A national coordinating body, or "apex group", potentially involving a public–private partnership, would provide strategic oversight and ensure alignment across jurisdictions. This type of approach respects the diversity of actors, technologies, and risks across the food system while promoting shared standards and coordinated security. It offers scalability, trust, and adaptability, especially important given the large number of small and mid-sized enterprises in the sector. Sector-specific working groups (e.g., for producers, processors, retailers, etc.) would contribute tailored guidance, while regional partners could support localized implementation through awareness building, training and outreach, and program implementation. A senior government official and an insurance industry leader suggested that, while there is a role for government, it should be as a partner, rather than a leader. The insurance participant recommended that "government should fund, not lead. . . let industry guide implementation." Core cybersecurity standards and best practices, adapted from existing guidelines and frameworks, would need to be developed collaboratively, with modular add-ons addressing sector-specific needs, such as IoT security in smart farming or data integrity in cold chains. Implementation could be supported by industry champions, shared knowledge hubs, and third-party certification options. This approach encourages shared responsibility, enables flexible risk management, and promotes opportunities for broad adoption, particularly among small and mid-sized enterprises, while maintaining coherence across the national food system.

Divergent views were expressed concerning the role government might play in relation to both leadership and legislating and enforcing standards at the level of the FVC. Some suggested that, because the cybersecurity of the FVC is a pan-Canadian concern, leadership from the federal government would be essential, and that this might be the only way to create a reasonable baseline of practice enhancements across this CI. Government was recognized as the only party capable of convening the necessary participants for a comprehensive development initiative, and of providing the incentives and enforcement needed to significantly enhance cybersecurity capacity across the FVC. An effective set of standards or guidelines would need to be seen as practical enablers of innovation, a marketing/trade advantage for agri-food businesses, and an achievable accomplishment for those who are currently lower in cyber maturity and resource capacity. Others, including a government participant, suggested a more tempered role for government. For example, were government to seek too prominent a role in cybersecurity standards

Figure 26: Overview of proposed governance model for a cybersecurity standards initiative serving the Canadian FVC.



development and implementation, it could be regarded as overreach and might lead to various unintended "backfire" effects. These differing views reflected not just pragmatic concerns, but also opposing philosophical viewpoints about the role of government in the broader agri-food sector. However, the overall sentiment of interviewees was that government could play a helpful role, supportive versus directive, within a collaborative cybersecurity standardization initiative.

What industry guidance might look like in practice varied across participants. For example, one participant working for a federation emphasized that industry alignment with cybersecurity standards and best practices should be entirely voluntary. Others suggested that voluntary frameworks, or standards controlled exclusively by industry, were seen by some as a recipe for inertia and persistent vulnerability. This divergence of perspectives represents an important tension to resolve, not just from the standpoint of creating an effective participatory process for managing a standards initiative, but also because the FVC is a CI, vital to the well-being of all Canadians. Although not reflected in participant suggestions, any process that centres on enhancing the safety, resilience, and sovereignty of the Canadian food system should also consider socio-economic factors [1], [210] that may impact various populations, including Indigenous communities and a range of equity-deserving groups. Representation from these non-traditional parties in standards development initiatives would support a more holistically informed process. In today's dynamic and rapidly evolving threat environment, the pressure on the Canadian FVC is intensifying, as are the positive roles it can play both domestically and globally. Therefore, an effective cybersecurity framework for this CI could benefit from incorporating the six design principles that were proposed in Section 3.5.15 of this report:

- Applicability. Standards or guidelines must address the widest array of cybersecurity threats, such as ransomware, advanced persistent threats, threats to IT and OT, and the increasingly prevalent issue of social engineering via synthetic media, such as deepfakes.

- Relevance. Standards must address real and perceived needs across a broad spectrum of users. This will ensure they resonate with both highly technical cybersecurity personnel and those with limited cybersecurity knowledge.
- Technical capacity and affordability. Determining the technical and financial capacity required to implement and monitor standards is crucial. This includes an assessment of the resources needed to effectively adopt, use, and evaluate the standards within an organization and across the FVC.
- Agility. The agility of standards and standards frameworks is paramount in allowing the sector to effectively contend with a rapidly evolving threat environment. Features that allow for flexibility in adapting to changes are essential.
- Shared development. Standards must be collaboratively developed with input from multiple relevant groups.
- Context. Standards must operate in a context that reflects both the specific needs of the FVC and the broader societal implications of cybersecurity.

The burden of additional training in cybersecurity risk management may be reduced by incorporating it into existing, accepted programs such as those focusing on occupational health and safety. Awareness building is perhaps the most important step towards enhanced cybersecurity across the FVC. A cybersecurity standards initiative could serve as a common point of focus around which several beneficial collaborations could coalesce. A federated type of governance model embodies the idea of shared responsibility, which is essential for grappling with the shared nature of CI risk. It offers the opportunity to balance interests in sectoral and local autonomy with the need for national coordination and system-wide benefits. It can support differing levels of attention and support, aligned to variability in cybersecurity maturity.

Notwithstanding the preceding focus on opportunities for standardization work to play a helpful role in strengthening cybersecurity preparedness and capacity across the FVC, it is important to understand that the main focus of current standards is typically on categorizations of vulnerabilities and local practices for addressing them. While standardization is a necessary component of building cybersecurity, it is not a sufficient approach for preventing malicious cyber events. An effective cybersecurity position for the FVC will require all of the preceding elements, as well as:

- A strong business case for adoption of standards and best practices;
- Methods for ensuring proper implementation of standards and best practices;
- Coordinated sharing of threat intelligence;
- Awareness building, shared learning; and
- Advancing individual and organizational capacity to participate in the development of greater cyber resilience.

4.2 Recommendations

To support the role of standardization in strengthening cybersecurity capacity across the FVC, the following actions, aligned with the previously proposed governance model (see Figure 26), are recommended for consideration.

1. Any interested party-based process of standardization should include not only the usual diversity of traditional (private and public sector) actors but also non-traditional parties to standardization initiatives (e.g., food security researchers, representatives from under-represented communities and equity-deserving groups, and those involved with Indigenous food security/food sovereignty). Such a diversified structure would support mutually reinforcing activities related to awareness, shared ownership and successful implementation [217].
2. Standardization work emphasizing the Canadian context should include the following activity clusters:
    a. Engage different FVC actors to encourage and leverage their capacity to support outreach and education, through trusted channels, on the central role of cybersecurity as a FVC business enabler and component of business risk management, and the role that standardization could play in strengthening cybersecurity, thereby socializing a receptive "constituency for change."

b. Develop tiered, modular cybersecurity standards/guidelines tailored to the differing levels of cyber maturity within the Canadian FVC, based on the six design principles proposed in this report. The standards might draw from existing guidelines, such as those from the CCCS, aligned with relevant families of standards and best practices (e.g., NIST, ISO), and responsive to the evolving realities of the Canadian context.

c. Identify, and pilot standards/guidelines within high-risk FVC subsectors and provinces willing to serve as test jurisdictions.

d. Encourage dialogue on opportunities to integrate cybersecurity best practices into widely used frameworks for food safety, traceability, and sustainability.

e. Through public–private–academic partnerships, embed and pilot cybersecurity components within existing education, business and employee training and certifications, such as occupational health and safety training.

f. Explore, assess, and encourage the inclusion of incentives for cybersecurity practice enhancements, where relevant and beneficial, into insurance, procurement, and grant frameworks to support adoption. Consider the roles and responsibilities of big equipment manufacturers and food retailers, as well as government, in enabling effective and sustainable adoption of standards and associated practices.

g. Identify options that might be included in regulatory and compliance frameworks, tied to the aforementioned incentives programs; clarify roles and responsibilities for various actors related to these.

h. Encourage and provide input to the establishment of mechanisms for safe, anonymized, breach reporting and threat intelligence sharing.

i. Engage levels of government to potentially incorporate:

- Cybersecurity as part of rural/regional economic development policies and programs and food sovereignty initiatives.
- Greater attention to the food CI in updates to Canada's National Cyber Security Strategy and CI defence plans.



j. Contribute to networked cybersecurity capacity across the FVC by expanding or adapting the elements of the cybersecurity framework for the agricultural sector [11] presented in this report by:

- Identifying opportunities to enable business-level cybersecurity through an appropriate mix of awareness, incentives, practical supports, and requirements;
- Identifying, promoting, and developing workforce capacity involving FVC cybersecurity (i.e., upskilling current FVC workforce; including cybersecurity as a key set of knowledge, skills, and abilities for new entrants to FVC careers; and promoting FVC careers/business opportunities for new and current cybersecurity practitioners);
- Fostering and sustaining cross-sector partnerships on cybersecurity within the FVC; and
- Encouraging alignment of cybersecurity policy, legislation, standards, governance, and incentives focusing on the FVC.

References

[1] S. Rotz et al., "The politics of digital agricultural technologies: A preliminary review," *Sociol. Rural.,* vol. 59, no. 2, pp. 203–229, 2019, https://doi.org/10.1111/soru.12233.

[2] Public Safety Canada. "Canada's critical infrastructure (CI)." [Online]. Available: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx

[3] Public Safety Canada, "National Cross Sector Forum: 2021–2023 action plan for critical infrastructure," Public Safety Canada, Ottawa, ON, Canada, 2021. [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/2021-ctn-pln-crtcl-nfrstrctr-en.pdf

[4] Public Safety Canada, "National strategy for critical infrastructure," Public Safety Canada, Ottawa, ON, Canada, 2009. [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx

[5] J. Botschner, C. Corley, E. Fraser, R. Kotak, and D. McMahon, "Cyber security in digital agriculture," Community Safety Knowledge Alliance, Ottawa, ON, Canada, 2021. [Online]. Available: https://cskacanada.ca/wp-content/uploads/2022/11/221028-CSKA-Cyber_Security_in_Agriculture-digital.pdf

[6] J. Botschner, C. Corley, E. Fraser, R. Kotak, and D. McMahon, "Cyber security capacity in Canadian agriculture: Research summary," Community Safety Knowledge Alliance, Ottawa, ON, Canada, Apr. 2022. [Online]. Available: https://cskacanada.ca/wp-content/uploads/2023/10/CSKA-CyAg-ResearchSummary.pdf

[7] A. G. Green et al., "A scoping review of the digital agricultural revolution and ecosystem services: Implications for Canadian policy and research agendas," *Facets,* vol. 6, no. 1, pp. 1955–1985, 2021, https://doi.org/10.1139/facets-2021-0017.

[8] J. Botschner, C. Corley, E. D. G. Fraser, R. Kotak, D. McMahon, and L. Newman, "Cyber security in digital agriculture: A national security risk?" in *(In)Security: Identifying the Invisible Disruptors of Security,* G. Adlakha-Hutcheon and C. Kelshall, Eds., London, UK: Springer Nature, 2024, pp. 281–315. [Online]. Available: https://doi.org/10.1007/978-3-031-67608-6_6

[9] V. Zatsu et al., "Revolutionizing the food industry: The transformative power of artificial intelligence–A review," *Food Chem. X,* vol. 24, 2024, Art. no. 101867, https://doi.org/10.1016/j.fochx.2024.101867.

[10] S. Purnama and W. Sejati, "Internet of things, big data, and artificial intelligence in the food and agriculture sector," *Int. Trans. Artif. Intell.,* vol. 1, no. 2, pp. 156–174, 2023. [Online]. Available: https://scispace.com/pdf/internet-of-things-big-data-and-artificial-intelligence-in-2yjsedab.pdf

[11] J. Botschner, C. Corley, E. Fraser, R. Kotak, and D. McMahon, "Cyber barn raising: A framework and recommendations for strengthening cyber resilience in Canadian agriculture," Community Safety Knowledge Alliance, Ottawa, ON, Canada, 2022. [Online]. Available: https://cskacanada.ca/wp-content/uploads/2024/05/240328-CSKA-CyberBarnRaising-web.pdf

[12] A. O. Adewusi, N. R. Chiekezie, and N. L. Eyo-Udo, "Cybersecurity threats in agriculture supply chains: A comprehensive review," *World Journal of Advanced Research and Reviews,* vol. 15, no. 3, pp. 490–500, 2022, https://doi.org/10.30574/wjarr.2022.15.3.0888.

[13] A. Yazdinejad, A. Dehghantanha, H. Karimipour, G. Srivastava, and R. M. Parizi, "A robust privacy-preserving federated learning model against model poisoning attacks," *IEEE Trans. Inf. Forensics Secur.,* vol. 19, pp. 6693–6708, 2024, https://doi.org/10.1109/TIFS.2024.3420126.

[14] J. Botschner and R. Kotak, "Creating a farm network topology map," Community Safety Knowledge Alliance, Ottawa, ON, Canada, 2023. [Online]. Available: https://cskacanada.ca/wp-content/uploads/2023/10/CSKA-Farm-Network-Typology-Mapping.pdf

[15] J. Botschner and R. Kotak, "Creating a farm business cyber security policy," Community Safety Knowledge Alliance, Ottawa, ON, Canada, 2023. [Online]. Available: https://cskacanada.ca/wp-content/uploads/2023/10/CSKA-Farm-Business-CyberSecurity-Policy.pdf

[16] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, M. Hammoudeh, H. Karimipour, and G. Srivastava, "Block hunter: Federated learning for cyber threat hunting in blockchain-based IIoT networks," *IEEE Trans. Ind. Inform.,* vol. 18, no. 11, pp. 8356–8366, 2022, https://doi.org/10.1109/TII.2022.3168011.

[17] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, and H. Karimipour, "Secure intelligent fuzzy blockchain framework: Effective threat detection in IoT networks," *Comput. Ind.,* vol. 144, 2023, Art. no. 103801, https://doi.org/10.1016/j.compind.2022.103801.

[18] A. Yazdinejad, M. Kazemi, R. M. Parizi, A. Dehghantanha, and H. Karimipour, "An ensemble deep learning model for cyber threat hunting in industrial internet of things," *Digit. Commun. Netw.,* vol. 9, no. 1, pp. 101–110, 2023, https://doi.org/10.1016/j.dcan.2022.09.008.

[19] A. Yazdinejad et al., "A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures," *Appl. Sci.,* vol. 11, no. 16, 2021, Art. no. 7518, https://doi.org/10.3390/app11167518.

[20] P. Veginadu, H. Calachem, M. Gussy, A. Pandian, and M. Masood, "An overview of methodological approaches in systematic reviews," *J. Evid. Based Med.,* vol. 15, no. 1, pp. 39–54, https://doi.org/10.1111/jebm.12468.

[21] M. Bamberger, J. Rugh, and L. Mabry, *Real World Evaluation: Working Under Budget, Time, Data and Political Constraints.* Thousand Oaks, CA, United States: Sage Publications, 2006.

[22] K. Charmaz, "Grounded theory: Objectivist and constructivist methods," in *Handbook of Qualitative Research,* 2nd ed. N. K. Denzin and Y. S. Lincoln, Eds., Thousand Oaks, CA, United States: Sage Publications, 2000, ch. 19, pp. 509–535.

[23] Agriculture Council of Saskatchewan, "Practical guide to value chains in Canada," Agriculture Council of Saskatchewan, Saskatoon, SK, Canada, 2013. [Online]. Available: https://agcouncil.ca/wp/wp-content/uploads/2017/03/ThePracticalGuide031213.pdf

[24] M. E. Porter, *Competitive Advantage: Creating and Sustaining Superior Performance,* New York, NY, United States: Free Press, 1985.

[25] E. Sweeney, "Supply chain management and the value chain," *Supply Chain Perspectives, Journal of the National Institute for Transport and Logistics,* vol. 10, no. 2, pp. 13–15, 2009. [Online]. Available: https://arrow.tudublin.ie/cgi/viewcontent.cgi?article=1075&context=nitloth

[26] S. K. Dubey, R. Singh, S. P. Singh, A. Mishra, and N. V. Singh, "A brief study of value chain and supply chain," in *Agriculture Development and Economic Transformation in Global Scenario,* R. K. Rao, Ed., Varanasi, India: Mahima Research Foundation and Social Welfare, ch. 25, pp. 177–183, 2020. [Online]. Available: https://www.researchgate.net/publication/344374264_A_BRIEF_STUDY_OF_VALUE_CHAIN_AND_SUPPLY_CHAIN

[27] 4AG Robotics. "Robots picking mushrooms." Accessed: May 5, 2025. [Online]. Available: https://4ag.ai/

[28] Vivid Machines. "Vivid Machines: Precision crop." Accessed: May 5, 2025. [Online]. Available: https://www.vivid-machines.com/

[29] Canadian Agri-Food Automation and Intelligence Network, "Pan-Canadian smart farm network development." [Online]. Available: https://caain.ca/our-projects/pan-canadian-smart-farm-network/

[30] EMILI. "Innovation farms." Accessed: Apr. 18, 2025. [Online]. Available: https://emilicanada.com/Innovation-Farms/

[31] T. R. C. Konfo, F. M. C. Djouhou, M. H. Hounhuigan, E. Dahouenon-Ahoussi, F. Avlessi, and C. K. D. Sohounhloue, "Recent advances in the use of digital technologies in agri-food processing: A short review," *Appl. Food Res.,* vol. 3, 2023, Art. no. 100329, https://doi.org/10.1016/j.afres.2023.100329.

[32] European Parliament and the Council of the European Union, Jan. 28, 2002. *Regulation (EC) No. 178/2002, laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety.* [Online]. Available: https://eur-lex.europa.eu/eli/reg/2002/178/oj

[33] Canadian Food Inspection Agency. "Food safety standards and guidelines." [Online]. Available: https://inspection.canada.ca/en/food-safety-industry/food-safety-standards-guidelines

[34] S. Senturk, F. Senturk, and H. Karaca, "Industry 4.0 technologies in agri-food sector and their integration in the global value chain: A review," *J. Clean. Prod.,* vol. 408, 2023, Art. no. 137096, https://doi.org/10.1016/j.jclepro.2023.137096.

[35] A. Mikhailov, G. F. Camboim, F. M. Reichert, and P. A. Zawislak, "The application and benefits of digital technologies for agri-food value chain: Evidence from an emerging country," *Rev. Admin. Mackenzie,* vol. 23, no. 5, pp. 1–29, 2022, https://doi.org/10.1590/1678-6971/eRAMR220114.en.

[36] R. K. Singh, R. Mishra, S. Gupta, and A. Mukherjee, "Blockchain applications for secured and resilient supply chains: A systematic literature review and future research agenda," *Comp. Ind. Eng.,* vol. 175, 2023, Art. no. 108854, https://doi.org/10.1016/j.cie.2022.108854.

[37] R. Prodanović et al., "Wireless sensor network in agriculture: Model of cyber security," *Sensors,* vol. 20, no. 23, 2020, Art. no. 6747, https://doi.org/10.3390/s20236747.

[38] T. Ojha, S. Misra, and N. S. Raghuwanshi, "Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges," *Comp. Electron. Agric.,* vol. 118, pp. 66–84, 2015, http://dx.doi.org/10.1016/j.compag.2015.08.011.

[39] Food Industry Executive, "2025 state of food manufacturing: Digital transformation," Food Industry Executive, Portland, OR, United States, 2025. [Online]. Available: https://marketing.foodindustryexecutive.com/hubfs/2025%20State%20of%20Food%20Manufacturing_%20Digital%20Transformation.pdf

[40] Arrell Food Institute and Food and Agriculture Institute, "Feeding the future with Canadian technology: Strategies and recommendations to support a thriving Canadian ag-tech ecosystem," Arrell Food Institute, University of Guelph, and Food and Agriculture Institute, University of the Fraser Valley, Sep. 2024. [Online]. Available: https://arrellfoodinstitute.ca/wp-content/uploads/2024/10/Ag-tech-Strategy-Report-Screen-revised-Oct-8.pdf

[41] M.-J. Bogaardt, K. Poppe, V. R. Viool, and E. van Zuidam, "Cybersecurity in the agrifood sector," Capgemini Consulting and Wageningen UR, The Netherlands, 2016. [Online]. Available: https://www.capgemini.com/consulting-nl/wp-content/uploads/sites/33/2017/08/02-029.16_agrifood_pov_consulting__web.pdf

[42] S. Wolfert, L. Ge, C. Verdouw, and M.-J. Bogaardt, "Big data in smart farming – A review," *Agric. Syst.,* vol. 153, pp. 69–80. 2017, https://doi.org/10.1016/j.agsy.2017.01.023.

[43] J. A. Tanimu and W. Abada, "Addressing cybersecurity challenges in robotics: A comprehensive overview," *Cyber Secur. Appl.,* vol. 3, 2025, Art. no. 100074, https://doi.org/10.1016/j.csa.2024.100074.

[44] A. Rogachev and E. Melikhova, "SCADA and GIS systems for monitoring and managing digital objects of agro-industrial production," in *Proc. of the XIII International Scientific Conference on Architecture and Construction 2020,* A. Mottaeva, Ed., vol. 130, 2020, pp. 725–734, https://doi.org/10.1007/978-981-33-6208-6_55.

[45] J. F. Holmes, G. Russell, and J. K. Allen, "Supervisory control and data acquisition (SCADA) and related systems for automated process control in the food industry: An introduction," in *Robotics and Automation in the Food Industry,* D. G. Caldwell, Ed., Cambridge, United Kingdom: Woodhead Publishing, 2013, ch. 6, pp. 130–142. [Online]. Available: https://doi.org/10.1533/9780857095763.1.130

[46] R. Maududy and A. M. Nurdin, "An architecture framework for supply chain management systems integrated with supervisory control and data acquisition," *J. Logist. Inform. Serv. Sci.,* vol. 11, no. 5, pp. 38–51, 2024, https://doi.org/10.33168/JLISS.2024.0503.

[47] J. Thyberg, "Guardians of the grid: A comparative study of best practices and experts' current approaches in cybersecurity for control systems," MSc Eng. thesis, Uppsala Univ., Faculty of Science and Technology, Systems in Technology and Society, Uppsala, Sweden, Jun. 2024. [Online]. Available: https://www.diva-portal.org/smash/get/diva2%3A1877106/FULLTEXT01.pdf

[48] A. Kulkarni, Y. Wang, M. Gopinath, D. Sobien, A. Rahman, and F. A. Batarseh, "A review of cybersecurity incidents in the food and agriculture sector," *J. Agric. Food Res.,* vol. 23, 2024, Art. no. 102245, https://doi.org/10.1016/j.jafr.2025.102245.

[49] Z. J. Chen and A. Jewitt. "Canadian agriculture at a glance: Canada's farms integrate renewable energy production and technologies toward a future of sustainable and efficient agriculture." Statistics Canada. [Online]. Available: https://www150.statcan.gc.ca/n1/pub/96-325-x/2021001/article/00016-eng.htm

[50] O. Bamisile et al., "Towards cleaner/sustainable energy consumption in agriculture farms: Performance assessment of two innovative high-performance solar-based multigeneration systems," *Energy Convers. Manag.,* vol. 244, 2021, Art. no. 114507, https://doi.org/10.1016/j.enconman.2021.114507.

[51] X. Yang et al., "A survey on smart agriculture: Development modes, technologies, and security and privacy challenges," *IEEE/CAA J. Autom. Sin.,* vol. 8, no. 2, pp. 273–302, 2021, https://doi.org/10.1109/JAS.2020.1003536.

[52] M. Amiri-Zarandi, M. Hazrati Fard, S. Yousefinaghani, M. Kaviani, and R. Dara, "A platform approach to smart farm information processing," *Agriculture,* vol. 12, no. 6, 2022, Art. no. 838, https://doi.org/10.3390/agriculture12060838.

[53] J. Wang and H. Yue, "Food safety pre-warning system based on data mining for a sustainable food supply chain," *Food Control,* vol. 73, pt. B, pp. 223–229, 2017, https://doi.org/10.1016/j.foodcont.2016.09.048.

[54] J. Zuo et al., "RFID-based sensing in smart packaging for food applications: A review," *Future Foods,* vol. 6, 2022, Art. no. 100198, https://doi.org/10.1016/j.fufo.2022.100198.

[55] C. Tomulescu, "Cyberbiosecurity. A short review," in *Proc. 8th Smart Cities Int. Conf. (SCIC),* Dec. 2020. [Online]. Available: https://www.scrd.eu/index.php/scic/article/view/352

[56] M. Fulton, M.-A. Pigeon, B. Oemichen, and Y. Yang, "Digital technologies and the big data revolution in the Canadian agricultural sector: Opportunities, challenges, and alternatives," Canadian Centre for the Study of Co-operatives, University of Saskatchewan, Saskatoon, SK, Canada, Aug. 2021. [Online]. Available: https://usaskstudies.coop/documents/big-data-in-canadian-agriculture-report-fultonetal.pdf

[57] K. Hiebert, D. Lussier, E. Lika, and T. McCann, "The future is digital: Digital agriculture and Canadian agriculture policy," Canadian Agri-Food Policy Institute, Ottawa, ON, Canada, 2025. [Online]. Available: https://capi-icpa.ca/wp-content/uploads/2025/05/2025-05-20-Digital-Agriculture-EN-CAPI.pdf

[58] T. Laugerette and F. Stöckel, "From agriculture to agtech: An industry transformed beyond molecules and chemicals," Monitor Deloitte, 2016. [Online]. Available: https://www.academia.edu/31462238/From_Agriculture_to_AgTech_An_industry_transformed_beyond_molecules_and_chemicals

[59] C. Cumo, "Book review: Ian Mosby, Sarah Rotz, and Evan D. G. Fraser, Uncertain harvest: The future of food on a warming planet," *Can. J. Hist.,* vol. 55, no. 3, pp. 325–327, 2020, https://doi.org/10.3138/cjh.55.3-br19.

[60] F. R. Batubara, J. Ubacht, and M. Janssen, "Challenges of blockchain technology adoption for e-government: A systematic literature review," in *Proc. of 19th International Conference on Digital Government Research: Governance in the Data Age (dg.o '18),* Delft, Netherlands, 2018, pp. 1–9, https://doi.org/10.1145/3209281.3209317.

[61] N. Etemadi, Y. Borbon-Galvez, and F. Strozzi, "Blockchain technology for cybersecurity applications in the food supply chain: A systematic literature review," presented at XXV Summer School "Francesco Turco" — Industrial Systems Engineering, Bergamo, Italy, Sep. 9–11, 2020. [Online]. Available: https://summerschool-aidi.it/images/papers/session_3_2020/ID-38.pdf

[62] H. Solomon. "Maple Leaf Foods confirms it was hit by ransomware, won't pay attackers." Channel Daily News. [Online]. Available: https://channeldailynews.com/news/maple-leaf-foods-confirms-it-was-hit-by-ransomware-wont-pay-attackers/79161

[63] Cyber Security Incident Database. "Cyber incident victim: Crystal Valley." [Online]. Available: https://www.csidb.net/csidb/incidents/a12b842a-0de3-4fdf-8533-f299cbb98eb7/

[64] La Presse canadienne. "L'UPA victime d'une cyberattaque, son directeur plaide pour plus de sécurité." Radio-Canada. [Online]. Available: https://ici.radio-canada.ca/nouvelle/1904289/upa-cyberattaque-hackers-pirates-brp-ross

[65] D. Martin. "Threat of agriculture-related cybercrime is rising." Farmtario.com. [Online]. Available: https://farmtario.com/news/threat-of-agriculture-related-cybercrime-is-rising/

[66] P. Withers. "Major Canadian grocery chain says cyberattack cost $25 million." CBC News. [Online]. Available: https://www.cbc.ca/news/canada/nova-scotia/sobeys-cyber-attack-25-million-1.6686838

[67] J. Montpetit and A. Leung. "Canada's food supply – under threat?" CBC News. [Online]. Available: https://www.cbc.ca/newsinteractives/features/agri-food-canada-hacking

[68] A. Sharma. "$5.9 million ransomware attack on farming cooperative may cause food shortage." Ars Technica. [Online]. Available: https://arstechnica.com/information-technology/2021/09/5-9-million-ransomware-attack-on-farming-co-op-may-cause-food-shortage/

[69] J. Panettieri. "AGCO ransomware cyberattack timeline: Details and recovery updates." MSSP Alert and CyberRisk Alliance. [Online]. Available: https://www.msspalert.com/news/agco-ransomware-cyberattack-timeline-details-and-recovery-updates

[70] Waqas. "White hat hacker at DefCon jailbreaks tractor to play Doom." Hack Read. [Online]. Available: https://hackread.com/defcon-hacker-jaikbreaks-tractor-play-doom-game/

[71] J. Edmiston. "Safety net: A flock of chickens, held for ransom — Growing cyberattacks on Canada's food system threaten disaster." Financial Post. [Online]. Available: https://financialpost.com/cybersecurity/growing-cyberattacks-canada-food-system-threaten-disaster

[72] R. McCrimmon and M. Matishak. "Cyberattack on food supply followed years of warnings." Politico. [Online]. Available: https://www.politico.com/news/2021/06/05/how-ransomware-hackers-came-for-americans-beef-491936

[73] J. Greig. "Stormous ransomware gang takes credit for attack on Belgian brewer Duvel." The Record. [Online]. Available: https://therecord.media/stormous-claims-duvel-beer-attack

[74] B. Toulas. "Dairy giant Agropur says data breach exposed customer info." Bleeping Computer. [Online]. Available: https://www.bleepingcomputer.com/news/security/dairy-giant-agropur-says-data-breach-exposed-customer-info/

[75] Freight Waves. "As ransomware attacks hit trucking, victims face costly dilemma." [Online]. Available: https://www.freightwaves.com/news/as-ransomware-attacks-hit-trucking-victims-face-costly-dilemma

[76] E. Kovacs. "Ransomware gang takes credit for Maple Leaf Foods hack." Security Week. [Online]. Available: https://www.securityweek.com/ransomware-gang-takes-credit-maple-leaf-foods-hack/

[77] L. Adriano. "Maple Leaf Foods confirms cyberattack, will not pay ransomware gang." Insurance Business. [Online]. Available: https://www.insurancebusinessmag.com/ca/news/cyber/maple-leaf-foods-confirms-cyberattack-will-not-pay-ransomware-gang-429218.aspx

[78] James. "8 recent cyber attacks on food production and agriculture." Wisdiam. [Online]. Available: https://wisdiam.com/publications/recent-cyber-attacks-food-agriculture-sector/

[79] Canadian Centre for Cyber Security, "National cyber threat assessment: 2025–2026," Communications Security Establishment Canada, Ottawa, ON, Canada, 2024. [Online]. Available: https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf

[80] L. Constantin. "REvil ransomware explained: A widespread extortion operation." CSO Online. [Online]. Available: https://www.csoonline.com/article/570101/revil-ransomware-explained-a-widespread-extortion-operation.html

[81] M. McIntosh. "Hog farm targeted by ransomware." Farmtario.com. [Online]. Available: https://farmtario.com/news/hog-farm-targeted-by-ransomware/

[82] EMILI Data Initiative. "Introduction to agricultural cybersecurity." [Online]. Available: https://emili-data-initiative.slite.page/p/vThTP2peZa6o4t/Introduction-to-Agricultural-Cybersecurity

[83] L. Manning and A. Kowalska, "The threat of ransomware in the food supply chain: A challenge for food defence," *Trends Organ. Crim.,* pp. 1–29, 2023. [Online]. Available: https://doi.org/10.1007/s12117-023-09516-y

[84] F. A. Gwelo, "Algorithmic bias and farmers' autonomy in AI-driven agricultural marketing and supply chains," in *AI and Machine Learning Applications in Supply Chains and Marketing,* R. Masengu, C. Tsikada, and J. Garwi, Eds., Hershey, PA: IGI Global Scientific Publishing, 2025, pp. 213–234. [Online]. Available: https://doi.org/10.4018/979-8-3693-6760-5.ch013

[85] M. Rowan. "AI bias and Canada's artificial intelligence and data act." Data Sentinel. [Online]. Available: https://www.data-sentinel.com/resources/ai-bias-and-canadas-artificial-intelligence-and-data-act

[86] N. Thomas, E. Chochla, and S. Lindsay, "Executive summary. Regulating AI: Critical issues and choices," Law Commission of Ontario, Toronto, ON, Canada, Apr. 2021. [Online]. Available: https://www.lco-cdo.org/wp-content/uploads/2021/04/LCO-Executive-Summary-Regulating-AI-Critical-Issues-and-Choices-Toronto-April-2021-1.pdf

[87] Innovation, Science and Economic Development Canada. "Artificial Intelligence and Data Act." [Online]. Available: https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act

[88] Innovation, Science and Economic Development Canada. "Canada's Digital Charter." [Online]. Available: https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world

[89] E. Fraser, L. Newman, and J. Botschner. "Canada's national security and the integrity of our food system go hand-in-hand." Hill Times. [Online]. Available: https://www.hilltimes.com/story/2022/01/04/canadas-national-security-and-the-integrity-of-our-food-system-go-hand-in-hand/270037/

[90] J. Nikander, O. Manninen, and M. Laajalahti, "Requirements for cybersecurity in agricultural communications networks," *Comput. Electron. Agric.,* vol. 179, 2020, Art. no. 105776, https://doi.org/10.1016/j.compag.2020.105776.

[91] Imperva. "OSI model." [Online]. Available: https://www.imperva.com/learn/application-security/osi-model/

[92] A. Triantafyllou, D. C. Tsouros, P. Sarigiannidis, and S. Bibi, "An architecture model for smart farming," in *15th Int. Conf. on Distributed Computing in Sensor Systems (DCOSS),* Santorini, Greece, 2019, pp. 385–392, https://doi.org/10.1109/DCOSS.2019.00081.

[93] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and privacy in smart farming: Challenges and opportunities," *IEEE Access,* vol. 8, pp. 34564–34584, 2020, https.//doi.org/10.1109/ACCESS.2020.2975142.

[94] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," presented at *6th International Conference on i-Warfare and Security (ICIW),* Washington, DC, United States, Mar. 17–18, 2011. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

[95] A. Hassanzadeh et al., "A review of cybersecurity incidents in the water sector," *J. Environ. Eng. ASCE,* vol. 146, no. 5, 2020, Art. no. 03120003, https://doi.org/10.1061/(ASCE)EE.1943-7870.0001686.

[96] Verizon. "Data breach investigations report." [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[97] D. Singh, A. Singh, M. Rakhra, T. Sarkar, G. Cheema, and A. Khamparia, "Predictions on the future of agriculture and recent developments in agricultural technology," in *The Smart IoT Blueprint: Engineering a Connected Future, Advances in Science, Technology & Innovation,* F. Al-Turjman, Ed., Switzerland: Springer Cham, 2024, pp. 297–303. [Online]. Available: https://doi.org/10.1007/978-3-031-63103-0_31

[98] Parliament of the United Kingdom, 2022. *Product Security and Telecommunications Infrastructure Act 2022,* c. 46. [Online]. Available: https://www.legislation.gov.uk/ukpga/2022/46/part/1/enacted

[99] Forbes. "Network segmentation: Top challenges and how to solve them." [Online]. Available: https://www.forbes.com/councils/forbestechcouncil/2024/05/29/network-segmentation-top-challenges-and-how-to-solve-them/

[100] E. Stone. "Update on right-to-repair." National Agricultural Law Center. [Online]. Available: https://nationalaglawcenter.org/update-on-right-to-repair/

[101] Colorado General Assembly, 2023. *Consumer Right To Repair Agricultural Equipment, HB23-1011.* [Online]. Available: https://www.leg.colorado.gov/bills/hb23-1011

[102] Parliament of Canada, 44th Parliament, 1st session, 2024. C-244, *An Act to amend the Copyright Act (diagnosis, maintenance and repair), Statutes of Canada 2024, c. 26.* [Online]. Available: https://www.parl.ca/legisinfo/en/bill/44-1/c-244

[103] C. Meyers, S. Powers, and D. Faissol, "Taxonomies of cyber adversaries and attacks: A survey of incidents and approaches," Lawrence Livermore National Laboratory, Livermore, CA, United States, Rep. LLNL-TR-419041, Apr. 2009. [Online]. Available: https://www.osti.gov/servlets/purl/967712

[104] EMILI. "Canadian Agri-Food Data Initiative: Free course provides core knowledge into data and digital technology." [Online]. Available: https://emilicanada.com/data-initiative/data-literacy/

[105] Parliament of Australia. "Bills Digest no. 28, 2024–25: Cyber Security Bill 2024 [and] Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024." [Online]. Available: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2425/25bd028

[106] Commonwealth of Australia, "Cyber security legislative reforms – Explanatory document: Cyber security (ransomware reporting) rules," Department of Home Affairs, Commonwealth of Australia, Canberra, Australia, 2023. [Online]. Available: https://www.cisc.gov.au/resources-subsite/Documents/cyber-security-ransomware-reporting-rules-explanatory-document.pdf

[107] A. Boghossian et al., "Threats to precision agriculture," 2018 Public-Private Analytic Exchange Program, Department of Homeland Security, Washington, DC, United States, 2018. [Online]. Available: https://doi.org/10.13140/RG.2.2.20693.37600

[108] H. Solomon. "Human error tops causes of data breaches, says Verizon report." IT World Canada. [Online]. Available: https://www.itworldcanada.com/article/human-error-tops-causes-of-data-breaches-says-verizon-report/48534

[109] S. Nifakos et al., "Influence of human factors on cyber security within healthcare organisations: A systematic review," *Sensors,* vol. 21, no. 15, 2021, Art. no. 5119, https://doi.org/10.3390/s21155119.

[110] S. N. Tambe-Jagtap, "Human-centric cybersecurity: Understanding and mitigating the role of human error in cyber incidents," *SHIFRA,* vol. 2023, pp. 53–59, 2023. https://doi.org/10.70470/SHIFRA/2023/007.

[111] B. Dupont, "The cyber-resilience of financial institutions: Significance and applicability," *J. Cybersecur.,* vol. 5, no. 1, 2019, Art. no. tyz013, https://doi.org/10.1093/cybsec/tyz013.

[112] B. Dupont, C. Shearing, and M. Bernier, "Withstanding cyber-attacks: Cyber-resilience practices in the financial sector," Global Risk Institute, Toronto, ON, Canada, Apr. 2020. [Online]. Available: https://globalriskinstitute.org/publication/withstanding-cyber-attacks-cyber-resilience-practices-in-the-financial-sector/

[113] D. Kahneman, *Thinking, Fast and Slow,* Toronto, ON, Canada: Doubleday Canada, 2011. [Online]. Available: https://www.penguinrandomhouse.ca/books/89308/thinking-fast-and-slow-by-daniel-kahneman/9780385676533

[114] K. M. Alnifie and C. Kim, "Appraising the manifestation of optimism bias and its impact on human perception of cybersecurity: A meta-analysis," *Journal of Information Security,* vol. 14, no. 2, pp. 93–110, 2023, https://doi.org/10.4236/jis.2023.142007.

[115] A. Dehghantanha and H. Karimpour, "Cybersecurity in smart farming: Canada market research," Cyber Science Lab, University of Guelph, ON, Canada, 2020. [Online]. Available: https://cybersciencelab.com/wp-content/uploads/2020/09/CybersecurityinAgReport.pdf

[116] C. Russell, J. Botschner, E. Duncan, A. Dehghantanha, and E. D. G. Fraser, "'I grow food, IT people do cybersecurity': Addressing cybersecurity risks in Canada's agri-food sector," *Smart Agric. Technol.,* vol. 10, 2025, Art. no. 100866, https://doi.org/10.1016/j.atech.2025.100866.

[117] D. Kahneman and A. Tversky, "Prospect theory: An analysis of decision under risk," *Econometrica,* vol. 47, no. 2, pp. 263–292, 1979, https://doi.org/10.2307/1914185.

[118] A. Bourgeois, "Cyberfraud in small business," Canadian Federation of Independent Business, Ottawa, ON, Canada, Feb. 2021. [Online]. Available: https://20336445.fs1.hubspotusercontent-na1.net/hubfs/20336445/research/Cyber-Fraud-in-Small-Business.pdf

[119] S. Russell, C. Jackson, and B. Cowles, "Cybersecurity budgeting: A survey of benchmarking research and recommendations to organizations," Centre for Applied Cybersecurity Research, Indiana University, Bloomington, IN, United States, Jun. 2016. [Online]. Available: https://hdl.handle.net/2022/22289

[120] M. P. Gallaher, B. R. Rowe, A. V. Rogozhin, and A. Link, "Economic analysis of cyber security," Air Force Research Laboratory, Rome, NY, United States, Rep. AFRL-IF-RS-TR-2006-227, Jul. 2006. [Online]. Available: https://www.researchgate.net/publication/235082256_Economic_Analysis_of_Cyber_Security

[121] NCX Group. "Under the microscope: Cybersecurity costs." [Online]. Available: https://ncxgroup.com/2021/08/cybersecurity-costs-under-the-microscope/

[122] Agriculture and Agri-Food Canada. "Overview of Canada's agriculture and agri-food sector." Accessed: Nov. 6, 2024. [Online]. Available: https://agriculture.canada.ca/en/sector/overview

[123] A. Frik, S. Egelman, M. Harbach, N. Malkin, and E. Peer, "Better late(r) than never: Increasing cyber-security compliance by reducing present bias," presented at Workshop on the Economics of Information Security, Innsbruck, Austria, Jun. 17–19, 2018. [Online]. Available: https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/06/WEIS_2018_paper_42.pdf

[124] Agriculture and Agri-Food Canada, "The Guelph Statement: A vision to 2028," Agriculture and Agri-Food Canada, Ottawa, ON, Canada, 2021. [Online]. Available: https://agriculture.canada.ca/sites/default/files/documents/2021-11/24172_fpt_policy_placemat_en_V15a.pdf

[125] United States Congress, 119th Congress, 1st Session, 2025. *Farm and Food Cybersecurity Act of 2025, S.754.* [Online]. Available: https://www.congress.gov/bill/119th-congress/senate-bill/754

[126] Global Cybersecurity Forum, "2024 cybersecurity workforce report: Bridging the workforce shortage and skills gap," Global Cybersecurity Forum, Riyadh, Saudi Arabia, 2024. [Online]. Available: https://web-assets.bcg.com/61/d3/705fbd684d70b0e5f98cdcf7cf47/2024-cybersecurity-workforce-report.pdf

[127] Strategic Advisory Group on Smart Farming, "Strategic Advisory Group Report on smart farming: Final report with recommendations," International Organization for Standardization, Geneva, Switzerland, Jan. 2023. [Online]. Available: https://www.iso.org/files/live/sites/isoorg/files/publications/en/2023_SAG-SF_Final_Report.pdf

[128] Public Safety Canada, "National cyber security action plan: 2019–2024," Public Safety Canada, Ottawa, ON, Canada, 2019. [Online]. Available: https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf

[129] Public Safety Canada, "National cyber security strategy 2019–2024: Report on the mid-term review," Public Safety Canada, Ottawa, ON, Canada, 2022. [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019-md-trm/index-en.aspx

[130] Agriculture and Agri-Food Canada. "Cyber security and your farming business." Accessed: Nov. 6, 2024. [Online]. Available: https://agriculture.canada.ca/en/programs/tools-manage-farm-risk-and-finance/cyber-security-and-your-farming-business

[131] Government of Canada. "Get cyber safe." Accessed: Oct. 30, 2024. [Online]. Available: https://www.getcybersafe.gc.ca/en

[132] Canadian Centre for Cyber Security. "Information for small and medium businesses." Accessed: Mar. 12, 2025. [Online]. Available: https://www.cyber.gc.ca/en/small-medium-businesses

[133] Community Safety Knowledge Alliance. "Cyber security capacity in Canadian agriculture." Accessed: Oct. 30, 2024. [Online]. Available: https://cskacanada.ca/projects/strengthening-the-cyber-security-capacity-of-canadas-agricultural-sector

[134] Government of Ontario. "Cybersecurity Preparedness Initiative." [Online]. Available: https://www.ontario.ca/page/cybersecurity-preparedness-initiative

[135] Government of British Columbia. "CyberBC: Advancing cybersecurity in BC with the broader public sector." [Online]. Available: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/cyber-bc

[136] University of Guelph. "Canada Cyber Foundry at University of Guelph." Accessed: Feb. 17, 2025. [Online]. Available: https://www.uoguelph.ca/ccf.

[137] Canadian Centre for Cyber Security, "Baseline cyber security controls for small and medium organizations," version 1.2, Communications Security Establishment, Ottawa, ON, Canada, 2020. [Online]. Available: https://www.cyber.gc.ca/sites/default/files/cyber/publications/Baseline.Controls.SMO1_.2-e%20.pdf

[138] Parliament of Canada, 44th Parliament, 1st Session, 2024. *Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts.* [Online]. Available: https://www.parl.ca/legisinfo/en/bill/44-1/c-26

[139] Canadian Centre for Cyber Security, "Cyber security readiness goals: Securing our most critical systems," version 1.0, Communications Security Establishment, Ottawa, ON, Canada, 2024. [Online]. Available: https://www.cyber.gc.ca/sites/default/files/cyber-readiness-goals-e.pdf

[140] Canadian Centre for Cyber Security. "Cyber security guidance: Annex 4A – Profile 1 – (PROTECTED B / Medium integrity / Medium availability) (ITSG-33)." [Online]. Available: https://www.cyber.gc.ca/en/guidance/annex-4a-profile-1-protected-b-medium-integrity-medium-availability-itsg-33

[141] E. Miscoi, D. G. C. Glover, and C. S. Morgan. "Bill C-26: Introduction of new mandatory breach reporting requirements in Canada." McCarthy Tétrault. [Online]. Available: https://www.mccarthy.ca/en/insights/blogs/techlex/bill-c-26-introduction-new-mandatory-breach-reporting-requirements-canada

[142] J. Cardy. "From Bill C-26 to Bill C-8: House of Commons reintroduces key cybersecurity legislation." Dentons. [Online]. Available: https://www.dentonsdata.com/from-bill-c-26-to-bill-c-8-house-of-commons-reintroduces-key-cybersecurity-legislation/

[143] Parliament of Canada, 45th Parliament, 1st session, 2025. *Bill C-8: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts.* [Online]. Available: https://www.parl.ca/legisinfo/en/bill/45-1/c-8

[144] Communications Security Establishment. "Top Canadian cyber security body releases flagship guidance for critical infrastructure." [Online]. Available: https://www.canada.ca/en/communications-security/news/2024/10/top-canadian-cyber-security-body-releases-flagship-guidance-for-critical-infrastructure.html

[145] Center for Internet Security, "NIST cybersecurity framework: Policy template guide," Multi-State Information Sharing and Analysis Center, Center for Internet Security, East Greenbush, NY, United States, 2019. [Online]. Available: https://CIS-MS-ISAC-NIST-Cybersecurity-Framework-Policy-Template-Guide-2024.pdf

[146] Cybersecurity and Infrastructure Security Agency. "Cross-sector cybersecurity performance goals." [Online]. Available: https://www.cisa.gov/cybersecurity-performance-goals

[147] Canadian Centre for Cyber Security, "Cross-sector cyber security readiness goals toolkit," Communications Security Establishment, Ottawa, ON, Canada, 2024. [Online]. Available: https://www.cyber.gc.ca/en/cyber-security-readiness/cross-sector-cyber-security-readiness-goals-toolkit

[148] Federal Bureau of Investigation, "Private Industry Notification: Smart farming may increase cyber targeting against US food and agriculture sector," Federal Bureau of Investigation, Washington, DC, United States, PIN 160331-001, Mar. 2016. [Online]. Available: https://nsarchive.gwu.edu/document/21674-document-09-federal-bureau-investigation

[149] Center for Internet Security. "CIS Critical Security Controls version 8." [Online]. Available: https://www.cisecurity.org/controls/v8

[150] Cybersecurity and Infrastructure Security Agency. "Cybersecurity threats to precision agriculture." [Online]. Available: https://www.cisa.gov/news-events/alerts/2018/10/03/cybersecurity-threats-precision-agriculture

[151] N. Marinos et al., "Critical infrastructure protection: Additional actions are essential for addressing cybersecurity framework adoption," United States Government Accountability Office, Washington, DC, United States, Rep. GAO 18-211, Feb. 2018. [Online]. Available: https://www.gao.gov/assets/d18211.pdf

[152] Executive Office of the President, 2021. *Improving the Nation's Cybersecurity, EO 14028, May 12, 2021.* [Online]. Available: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[153] United States Congress, 118th Congress, 2023. *Promoting Precision Agriculture Act of 2023, H.R.1697.* [Online]. Available: https://www.congress.gov/bill/118th-congress/house-bill/1697

[154] Cybersecurity and Infrastructure Security Agency. "Cyber Storm: Securing cyber space." [Online]. Available: https://www.cisa.gov/resources-tools/programs/cyber-storm

[155] Wikipedia. "Cyber-security regulation." Accessed Nov. 1, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Cyber-security_regulation

[156] European Union Agency for Cybersecurity. "NIS Directive 2. 2024." [Online]. Available: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/nis-directive-2

[157] NIS2 Directive. "NIS2 requirements." [Online]. Available: https://nis2directive.eu/nis2-requirements/

[158] J. Apostle and O. Hardan. "NIS2: Where do European countries stand on implementing cybersecurity strategies?" Orrick.com. [Online]. Available: https://www.orrick.com/en/Insights/2024/10/NIS2-Where-do-European-Countries-Stand-on-Implementing-Cybersecurity-Strategies

[159] F. Pop and L. Centeno Casado. "The NIS2 Directive: The road map to strengthen cybersecurity across the EU." European Institute of Public Administration. [Online]. Available: https://www.eipa.eu/blog/the-nis2-directive-the-road-map-to-strengthen-cybersecurity-across-the-eu/

[160] World Bank Open Data. "Agriculture, forestry, and fishing, value added (% of GDP)." [Online]. Available: https://data.worldbank.org/indicator/NV.AGR.TOTL.ZS

[161] European Union Cybersecurity Certification. "EU cybersecurity certification scheme on common criteria (EUCC)." 2024b. [Online]. Available: https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

[162] Farmers Guide. "Cyber security advice for farmers." [Online]. Available: https://www.farmersguide.co.uk/business/farm-security/cyber-security-advice-for-farmers/

[163] National Cyber Security Centre. "Cyber security advice for small to medium sized organisations." [Online]. Available: https://www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations

[164] Prime Minister's Office, "The King's speech 2024," Prime Minister's Office, London, United Kingdom, Jul. 2024. [Online]. Available: https://assets.publishing.service.gov.uk/media/6697f5c10808eaf43b50d18e/The_King_s_Speech_2024_background_briefing_notes.pdf

[165] P. Muncaster. "UK government set to introduce new cyber security and resilience bill." Infosecurity Magazine. [Online]. Available: https://www.infosecurity-magazine.com/news/government-cyber-security-bill-2024/

[166] Information Commissioner's Office. "The guide to NIS." [Online]. Available: https://ico.org.uk/for-organisations/the-guide-to-nis/

[167] European Parliament and the Council of the European Union, Jul. 6, 2016. *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.* [Online]. Available: http://data.europa.eu/eli/dir/2016/1148/oj

[168] House of Commons, "Product Security and Telecommunications Infrastructure Bill: Explanatory notes," House of Commons, London, United Kingdom, May 2022. [Online]. Available: https://publications.parliament.uk/pa/bills/cbill/58-03/0003/en/220003en.pdf

[169] *Cyber Security for Consumer Internet of Things: Baseline Requirements,* ETSI EN 303 645, version 2.1.1, European Telecommunications Standards Institute, Sophia Antipolis, France, 2020. [Online]. Available: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[170] National Coordinator for Counterterrorism and Security, "The Netherlands cybersecurity strategy 2022-2028," National Coordinator for Counterterrorism and Security, The Hague, Netherlands, 2022. [Online]. Available: https://english.nctv.nl/documents/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028

[171] Commonwealth of Australia, "2023–2030 Australian cyber security strategy: Action plan," Commonwealth of Australia, Department of Home Affairs, Commonwealth of Australia, Canberra, Australia, 2023. [Online]. Available: https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy-action-plan.pdf

[172] Corrs Chambers Westgarth. "'Shields' and 'horizons': Key takeaways from the 2023-2030 Australian Cyber Security Strategy." [Online]. Available: https://www.corrs.com.au/insights/shields-and-horizons-key-takeaways-from-the-2023-2030-australian-cyber-security-strategy

[173] Australian Signals Directorate. "Essential eight explained." [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-explained

[174] Charles Stuart University. "Farmers' guide to cybersecurity." [Online]. Available: https://www.csu.edu.au/research/farmers-cybersecurity

[175] National Cyber Security Centre. "NCSC cyber security framework." [Online]. Available: https://www.ncsc.govt.nz/resources/ncsc-cyber-security-framework?url=resources%2Fncsc-cyber-security-framework%2F

[176] National Institute of Standards and Technology. "Cybersecurity framework." [Online]. Available: https://www.nist.gov/cyberframework

[177] A. Calder, *NIST Cybersecurity Framework: A Pocket Guide.* Cambridgeshire, United Kingdom: IT Governance Publishing, 2018. [Online]. Available: https://doi.org/10.2307/j.ctv4cbhfx

[178] *Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements,* ISO/IEC 27001, International Organization for Standardization, Geneva, Switzerland, 2022. [Online]. Available: https://www.iso.org/standard/27001

[179] A. Calder, *ISO27001/ISO27002: A Pocket Guide,* 2nd ed. Cambridgeshire, United Kingdom: IT Governance Publishing, 2013. [Online]. Available: https://doi.org/10.2307/j.ctt5hh4qg

[180] *Security Techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management — Requirements and Guidelines,* ISO/IEC 27701, International Organization for Standardization, Geneva, Switzerland, 2019. [Online]. Available: https://www.iso.org/standard/71670.html

[181] *Information Security, Cybersecurity and Privacy Protection - Requirements for Bodies Providing Audit and Certification of Information Security Management Systems — Part 1: General,* CSA ISO/IEC 27006-1, Canadian Standards Association, Toronto, ON, Canada, 2025. [Online]. Available: https://www.csagroup.org/store/product/2431858

[182] *Cybersecurity — Supplier Relationships — Part 2: Requirements,* CSA ISO/IEC 27036-2, Canadian Standards Association, Toronto, ON, Canada, 2023. [Online]. Available: https://www.csagroup.org/store/product/CSA%20ISO-IEC%2027036-2%3A23

[183] *Information Technology — Information Security Incident Management — Part 1: Principles and Process,* CSA ISO/IEC 27035-1, Canadian Standards Association, Toronto, ON, Canada, 2024. [Online]. Available: https://www.csagroup.org/store/product/CSA_ISO-IEC_27035-1%3A24

[184] *Information Security, Cybersecurity and Privacy Protection — Guidance on the Integrated Implementation of ISO/IEC 27001 and ISO/IEC 20000-1,* CSA ISO/IEC 27013, Canadian Standards Association, Toronto, ON, Canada, 2022. [Online]. Available: https://www.csagroup.org/store/product/CSA%20ISO-IEC%2027013%3A22

[185] *Information Security, Cybersecurity and Privacy Protection — Application of ISO 31000:2018 for Organizational Privacy Risk Management,* CSA ISO/IEC 27557, Canadian Standards Association, Toronto, ON, Canada, 2024. [Online]. Available: https://www.csagroup.org/store/product/CSA_ISO-IEC_27557%3A24

[186] *Information Technology — Information Security Incident Management — Part 2: Guidelines to Plan and Prepare for Incident Response,* CSA ISO/IEC 27035-2, Canadian Standards Association, Toronto, ON, Canada, 2024. [Online]. Available: https://www.csagroup.org/store/product/CSA_ISO-IEC_27035-1%3A24

[187] *Cybersecurity — Supplier Relationships — Part 1: Overview and Concepts,* CSA ISO/IEC 27036-1, Canadian Standards Association, Toronto, ON, Canada, 2022. [Online]. Available: https://www.csagroup.org/store/product/CSA%20ISO-IEC%2027036-1%3A22

[188] *Information Technology — Security Techniques — Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services,* ISO/IEC 27017, International Organization for Standardization, Geneva, Switzerland, 2015. [Online]. Available: https://www.iso.org/standard/43757.html

[189] *Information Security, Cybersecurity and Privacy Protection — Guidelines for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors,* ISO/IEC 27018, International Organization for Standardization, Geneva, Switzerland, 2025. [Online]. Available: https://www.iso.org/standard/27018

[190] International Society of Automation. "ISA/IEC 62443 series of standards." [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[191] Fortinet. "IEC 62443 Standard: An Overview." [Online]. Available: https://www.fortinet.com/resources/cyberglossary/iec-62443

[192] International Society of Automation (ISA) Global Cybersecurity Alliance, "Security of industrial automation and control systems: An overview of ISA/IEC 62443 standards," ISA Global Cybersecurity Alliance, Research Triangle Park, NC, United States, 2025. [Online]. Available: https://isagca.org/hubfs/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf

[193] *Security for Industrial Automation and Control Systems – Part 1-5: Scheme for IEC 62443 Security Profiles,* IEC TS 62443-1-5, International Electrotechnical Commission, Geneva, Switzerland, 2023. [Online]. Available: https://cdn.standards.iteh.ai/samples/104529/06fcef24e4104218a1a5142ae0177bab/IEC-TS-62443-1-5-2023.pdf

[194] Office of the Superintendent of Financial Institutions. "OSFI releases final Guideline B-13 – Technology and Cyber Risk Management – Letter." [Online]. Available: https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/osfi-releases-final-guideline-b-13-technology-cyber-risk-management-letter-2022

[195] P. Hanycz, "Are Canadian cybersecurity-related laws sufficient to deal with the reality of today's threats," *Mathematics and Computer Science Capstones,* no. 45, 2019. [Online]. Available: https://digitalcommons.lasalle.edu/mathcompcapstones/45

[196] L. Brodsky and L. Oakes. "Data sharing and open banking." McKinsey & Company. [Online]. Available: https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking

[197] S. S. Khandke and T. Mayes, "HACCP implementation: A practical guide to the implementation of the HACCP plan," *Food Control,* vol. 9, no. 2–3, pp. 103–109, 1998, https://doi.org/10.1016/S0956-7135(97)00065-0.

[198] Canadian Institute of Food Safety. "What is HACCP?" [Online]. Available: https://www.foodsafety.ca/haccp-programs/what-is-haccp

[199] K. Liivat. "HACCP principles explained: What are the 7 HACCP principles?" FoodDocs. [Online]. Available: https://www.fooddocs.com/post/haccp-principles

[200] PCI Security Standards Council. "Securing the future of payments: PCI SSC publishes PCI Data Security Standard v4.0." [Online]. Available: https://www.pcisecuritystandards.org/about_us/press_releases/securing-the-future-of-payments-pci-ssc-publishes-pci-data-security-standard-v4-0/

[201] Association of International Certified Professional Accountants and Chartered Institute of Management Accountants. "SOC 2® – SOC for service organizations: Trust services criteria." Accessed: Nov. 1, 2024. [Online]. Available: https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2

[202] Information Systems Audit and Control Association. "COBIT: Effective IT governance at your fingertips." [Online]. Available: https://www.isaca.org/resources/cobit

[203] Chief Information Officer, U.S. Department of War. "Cybersecurity maturity model certification." [Online]. Available: https://dodcio.defense.gov/CMMC/

[204] K. Boeckl et al., "NISTIR 8228: Considerations for managing internet of things (IoT) cybersecurity and privacy risks," National Institute of Standards and Technology, Gaithersburg, MD, United States, 2019. [Online]. Available: https://doi.org/10.6028/NIST.IR.8228

[205] Federal Risk and Authorization Management Program. "FedRAMP® provides a standardized, reusable approach to security assessment and authorization for cloud service offerings." [Online]. Available: https://www.fedramp.gov/

[206] A. Natale, T. Poppensieker, and M. Thun. "From risk management to strategic resilience." McKinsey & Company. [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/from-risk-management-to-strategic-resilience

[207] L. H. Newman. "Ex-NSA chief Paul Nakasone has a warning for the tech world." WIRED. [Online]. Available: https://www.wired.com/story/ex-nsa-chief-paul-nakasone-has-a-warning-for-the-tech-world/

[208] S. J. Shackelford and Z. Bohm, "Securing North American critical infrastructure: A comparative case study in cybersecurity regulation," *Canada-United States Law Journal,* vol. 40, no. 1, pp. 145–170, 2016. [Online]. Available: https://scholarlycommons.law.case.edu/cuslj/vol40/iss1/9

[209] Canadian Centre for Cyber Security, "National Cyber Threat Assessment: 2025–2026," Communications Security Establishment, Ottawa, ON, Canada, 2025. [Online]. Available: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

[210] S. Singh, R. Vaishnav, S. Gautam, and S. Banerjee, "Agricultural robotics: A comprehensive review of applications, challenges and future prospects," in *Proc. of 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA),* Namakkal, India, 2024, pp. 1–8, https://doi.org/10.1109/AIMLA59606.2024.10531517.

[211] S. Gossett, A. Rodriguez, and E. Glover. "19 agricultural robots and farm robots you should know." Builtin.com. [Online]. Available: https://builtin.com/robotics/farming-agricultural-robots

[212] S. Lemke and T. Delormier, "Indigenous Peoples' food systems, nutrition, and gender: Conceptual and methodological considerations," *Matern. Child Nutr.,* vol. 13, no. S3, 2017, Art. no. e12499, [Online]. Available: https://doi.org/10.1111/mcn.12499

[213] S. Penner, K. Kevany, and S. Longboat, "Indigenous food sovereignty in Canada: Policy paper 2019," Rural Policy Learning Commons, 2019. [Online]. Available: https://rplcarchive.ca/wp-content/uploads/2019/02/Penner-Kevany-Longboat-2019-Indigenous-Food-Sovereignty-in-Canada-Policy-Brief.pdf

[214] Y. Jiang, M. A. Jeusfeld, M. Mosaad, and N. Oo, "Enterprise architecture modeling for cybersecurity analysis in critical infrastructures — A systematic literature review," *Int. J. Crit. Infrastruct. Prot.,* vol. 46, 2024, Art. no. 100700, https://doi.org/10.1016/j.ijcip.2024.100700.

[215] House of Commons Canada, "Protecting Canada's food system: Report of the Standing Committee on Public Accounts," Speaker of the House of Commons, Ottawa, ON, Canada, May 2022. [Online]. Available: https://publications.gc.ca/collections/collection_2022/parl/xc16-1/XC16-1-1-441-14-eng.pdf

[216] D. Namakshenas, A. Yazdinejad, A. Dehghantanha, and G. Srivastava, "Federated quantum-based privacy-preserving threat detection model for consumer Internet of Things," *IEEE Trans. Consum. Electron.,* vol. 70, no. 3, pp. 5829–5838, 2024, https://doi.org/10.1109/TCE.2024.3377550.

[217] F. Hanleybrown, J. Kania, and M. Kramer. "Channeling change: Making collective impact work." Stanford Social Innovation Review. [Online]. Available: https://ssir.org/articles/entry/channeling_change_making_collective_impact_work

[218] K. Burchardi, D. Nath, and J. Lan, "Federated data governance model: Critical path for organization data maturity transformation journey," Boston Consulting Group, Boston, MA, United States, 2024. [Online]. Available: https://media-publications.bcg.com/Federated-Data-Governance-Model.pdf

Appendix A: Question Guide for Semi-Structured Interviews with FVC Actors

Cybersecurity Risks

First, let's talk about your perspective on cybersecurity in the food value chain.
[Refer to Attachment A list if necessary, as a prompt]

1. I'd like to start by asking you to tell me about **your use of digital technologies** in the work you do or that your organization supports.

2. Are there any **specific cybersecurity vulnerabilities in the food value chain** that stand out to you as being the most important to address?

   [Refer to Attachment A list if necessary, as a prompt]

   - Why?

3. What kinds of **cyber threats** do you think are most likely to cause harm to our food system?

   [Refer to Attachment B list if necessary, as a prompt]

   - Why?

4. What are the **most serious impacts** that could result from this combination of vulnerabilities and threats?

   [Refer to Attachment C list if necessary, as a prompt]

   - Where, in the food value chain would these be most likely to happen? (e.g., stages of production, distribution, processing, etc.; specific commodity/food and beverage subsectors)
   - How likely do you think this is?

5. Thinking about the vulnerabilities, threats and impacts you just talked about, how would you describe the **overall level of cyber risk** the Canadian food value chain is facing right now?

   - How exposed would you say the food value chain is to cyber risks, compared to other parts of the economy?
   - Are there any differences that you're aware of across food value chain components — such as: primary production; distribution; processing; retail?
   - What do you think is behind these differences?
   - How concerned are you about this?

6. **How much of a priority do you think this should be** for the food system to address?

   - Why do you say that?

7. Is there **anyone helping to make a difference** in this space, right now?
   - What are they doing that's helpful?
   - What more, if anything, could be done?

8. Which organizations/stakeholders, in the food value chain, do you think are **best positioned** to provide leadership in making the system more cyber secure?

9. Which of these do you think should have the **most responsibility** for doing this? Who should pay for this?

A. Need for Cybersecurity Standards

Now, let's talk about the potential value of having a set of specific cybersecurity standards for the Canadian food value chain. Let me re-cap what we mean when we say cybersecurity standards:

> *These are guidelines and best practices designed to protect digital systems and information from cyber threats like hacking, data breaches, or malware. They can provide a framework for manufacturers to ensure their products are secure against tampering, and by organizations to secure their networks, software, and data, so they can operate safely and protect sensitive information. These standards help keep digital systems reliable and reduce the risk of cyberattacks.*

By way of example, some general purpose standards frameworks include [have brief description of each available if needed] Note that some of these frameworks are not strictly related to cybersecurity:

- **ISO/IEC 27001** (International Standards Organization/International Electrotechnical Commission, Information Security Management Systems): ISO/IEC 27001 provides a comprehensive framework for managing information security risks applicable to any organization, including those in smart farming and precision agriculture.
- **ISO/IEC 27017 and 27018** (Privacy Information Management System): These provide guidelines for information security controls applicable to the provision and use of cloud services (ISO/IEC 27017); and focus on protecting personal data in cloud and computing environments (ISO/IEC 27018:2019).
- **NIST** (National Institute of Standards and Technology): This is a comprehensive set of guidelines designed to help organizations manage and reduce cybersecurity risks.
- **ISA/IEC 62443 Series** (Industrial Communication Networks – Network and System Security): This set of standards outline a set of best practices for the implementation, maintenance and evaluation of electronically secure industrial automation and control systems.
- **OFSI** (Office of the Superintendent of Financial Institutions): This framework is designed to enhance the resilience of these institutions against cyber threats and ensure the stability of this critical infrastructure.
- **HACCP** (Hazard Analysis Critical Control Points): This framework is a systematic approach to ensuring food safety by identifying, evaluating, and controlling hazards that could compromise the safety of food products.
- **IoT Security Guidelines:** These focus on cybersecurity and privacy risks related to the use of IoT devices as distinct from conventional IT devices. The focus of these high-level guidelines is on protecting device-level security, data security and privacy.
- **PCI DSS (**Payment Card Industry Data Security Standard): This is applicable to organizations that handle branded credit cards.

10. In light of the cybersecurity landscape of the food value chain we just discussed, what gaps or issues do you think standards might be able to address?

11. Currently, there are no cybersecurity standards specific to the food value chain available, either internationally, or in Canada. Do you have any idea why this might be the case?

12. How familiar are you with the use of cybersecurity standards frameworks in any areas of the food value chain?

- Which standards?
- What areas?/What do these standards focus on?
- How would you describe their value to the food value chain, as a whole?

B. What Cybersecurity Standards Should Emphasize

13. What role do you think cybersecurity standards developed for the food value chain could play in helping this system be more cyber prepared?/In what ways could having system-specific cybersecurity standards help?

- What do you see as the most important benefits of having specific standards for the food value chain?
- Which cybersecurity risks could be better addressed by having specific cybersecurity standards for the food value chain, rather than using more general cybersecurity standards?
- How important is it to have cybersecurity standards tailored specifically to the needs of the food value chain?

14. Are there particular components of the food value chain where you think sector-specific cybersecurity standards could have the greatest impact?

- What are these?
- Why?

15. While national-level standards may be essential for addressing the unique needs within a specific jurisdiction, excessive focus on the development of national-level standards may result in fragmentation and duplication of effort. As such, in addition to the discussion of general vs FVC-specific standards, what are your perspectives on the need for Canada-specific vs international standards for this sector?

16. What kinds of digital items, activities or processes should a set of cybersecurity standards for the food value chain prioritize for greater security?

17. Are there specific areas in the food value chain that need more cybersecurity focus (e.g., IoT devices, information technology vs operational technology, precision farming, processing or manufacturing tools, business management software, networking technology, data governance, privacy)?

18. Are there specific parts of the broader context in which the food value chain operates that should be considered as a focus for standards [Consider, e.g.: climate related issues, geo-political threat actors, trade disruptions, enablers of collaboration through information sharing, enablers of response capacity through mechanisms that account for operations that have a mix of streams of proprietary data.]

C. Developing and Implementing Standards

19. What are the barriers that might interfere with a successful standards initiative (e.g., developing, implementing, auditing, scope management, national vs international standards setting, etc.)?

[Refer to Attachment D list if helpful]

- How might these be addressed?

20. Is there any particular individual or organization that you believe would be essential to be involved in developing these standards? Who?/Which organization?

21. What role would you see for people like you, or organizations that represent you within the food value chain in such a process?

22. Who should be responsible for maintaining and promoting these standards?

- What role might you see in this for provincial and federal governments?

23. Let's talk about some of the things that might need to be in place to support the effective use of these standards. Some of these could include:

- Promotion and awareness
- Education and training
- Funding and financial incentives
- Policy/legislation/regulation
- Other types of supports

In your view, what are the key enablers of a successful roll-out of cybersecurity standards for the food sector? Why?

Attachment A: List of Potential Cybersecurity Vulnerabilities

- **Outdated software and systems:** Using old technology that lacks security updates.
- **Weak passwords and authentication:** Poor or easily guessed passwords that allow unauthorized access.
- **Unsecured Internet of Things (IoT) devices:** Networked farm equipment or sensors that are not properly protected.
- **Unpatched vulnerabilities:** Failing to install security updates that fix known problems.
- **Inadequate data encryption:** Data that is not properly secured, making it easy for attackers to intercept.
- **Insufficient network security:** Weak protection for networks, such as lacking firewalls or intrusion detection systems.
- **Lack of physical security:** Inadequate measures to protect equipment from being accessed or tampered with physically.
- **Remote access vulnerabilities:** Weak security for remote systems, like allowing remote connections without proper safeguards.
- **Poor supply chain security:** Working with suppliers or partners who have weak cybersecurity practices.
- **Insufficient employee training:** Staff who are not aware of cybersecurity risks or how to prevent them.
- **Malware susceptibility:** Systems that are not protected against malicious software.

Attachment B: List of Potential Cybersecurity Threats

- **Botnets:** Groups of connected devices/software that can be controlled remotely
- **Cloud computing exploits:** Making use of features of cloud platforms to propagate malicious exploits, at-scale, to other systems connected through a cloud environment.
- **Cloud data leakage:** The unauthorized exposure of data pertaining to an organization's users or its services, leading to a violation of user or party privacy.
- **Cyber terrorism:** Using IoT systems and cyber-physical devices to attack businesses, systems or people for violent ideological purposes.
- **Data fabrication:** Creating malicious data or processes by misusing access provided for different purposes.
- **Data leakage:** Illegal transmission of an organization's data by an internal source (either a person or device) to an external destination.
- **Denial of service (DoS):** Uses various methods to deny access to a communication channel or a network component (e.g., server).
- **False data injection:** Supplying malicious information or control commands to a system.
- **Invalidation and compliance:** Using fabricated data to disrupt a valid certification of a process or transmission.
- **Malware injection:** Installation of malicious code within various elements (e.g., devices) within a system.
- **Man-in-the middle attacks:** Stealth based interception of communications between two or more parties.
- **Misconfiguration:** Configuring reporting systems to reflect invalid information about the management of an operation, to misdirect business critical decisions.
- **Misdirection (SQL injection):** Insertion of malicious code into a website's database through a form or input field, like a search box or login form.
- **Radio frequency jamming:** Interfering with the performance of a wireless network.
- **Ransomware:** Gaining illegal access to a system and encrypting critical digital assets, until a ransom is paid by the affected organization/individual, at which time a decryption key will be provided.
- **Side channel attacks:** Monitoring physical parameters to gather unauthorized information on system behaviour.
- **Software update attack:** Disrupting update processes of currently installed software.
- **Third party infiltration:** Infiltrating a system through an outside partner or provider who has access to the system and/or its data.

Attachment C: List of Potential Cybersecurity Impacts

- **Operational disruptions:** Cyberattacks on critical systems can halt farm operations, food processing, or distribution, leading to delays and financial losses.
- **Data theft and loss:** Hackers may steal or corrupt sensitive data, such as crop yield information, supply chain logistics, or proprietary research, impacting competitiveness and privacy.
- **Supply chain breakdowns:** A breach affecting one part of the food value chain can disrupt the entire system, causing delays in getting food to market.
- **Financial losses:** Cyber incidents can result in direct financial costs from ransom payments, system repairs, or revenue loss due to downtime.

- **Food safety risks:** Manipulation of data in automated systems that monitor food quality and safety could lead to contaminated or unsafe food reaching consumers.
- **Loss of consumer trust:** Data breaches or disruptions can damage the reputation of companies and undermine public confidence in food safety and reliability.
- **Theft of intellectual property:** Attackers may steal proprietary farming methods, product formulations, or genetic research, affecting innovation and competitiveness.
- **Compromise of precision agriculture:** Hacking of precision agriculture systems (like GPS-driven tractors or automated irrigation) can result in crop losses or reduced efficiency.
- **Increased insurance costs:** As cyber threats grow, insurance premiums for companies within the food value chain may rise, impacting overall profitability.
- **Regulatory and legal consequences:** Failing to protect against cyber risks can lead to legal penalties, fines, or stricter regulations, especially if consumer or environmental safety is compromised.

Attachment D: List of Potential Barriers to Cybersecurity Standards Development

- **Lack of stakeholder consensus:** Difficulty in getting agreement among diverse stakeholders with varying interests and priorities
- **Rapidly evolving technology:** Keeping up with fast-paced changes in technology and emerging threats
- **Limited resources:** Insufficient funding, time, or expertise dedicated to developing and implementing standards
- **Complexity of the food value chain:** The wide range of systems, practices, and actors makes it challenging to create one-size-fits-all standards
- **Resistance to change:** Reluctance from stakeholders to adopt new practices or invest in cybersecurity measures
- **Regulatory hurdles:** Navigating differing national and international regulations that can complicate standardization
- **Lack of awareness or understanding:** Limited understanding of cybersecurity risks among some stakeholders in the sector
- **Integration with existing processes:** Difficulty in aligning new cybersecurity standards with current practices and technologies
- **Economic constraints:** Concerns about the cost of implementing and maintaining cybersecurity measures
- **Data sharing concerns:** Worries about data privacy and the security of shared information among partners in the value

CSA Group Research

In order to encourage the use of consensus-based standards solutions to promote safety and encourage innovation, CSA Group supports and conducts research in areas that address new or emerging industries, as well as topics and issues that impact a broad base of current and potential stakeholders. The output of our research programs will support the development of future standards solutions, provide interim guidance to industries on the development and adoption of new technologies, and help to demonstrate our on-going commitment to building a better, safer, more sustainable world.

CSA GROUP™

© 2026 Canadian Standards Association. All Rights Reserved.