Intelligence Brief

The Exposed Field:

Why Agritech Has Become a Preferred Target and What Operations Leaders Can Do About It

WHITE TUQUE

Every Company
Cyber Resilient

Table of Contents

About Us

White Tuque is a Canadian boutique cybersecurity consultancy working with organizations in regulated, operationally complex industries to assess risk, close gaps, and build security programs that hold up under real production conditions.

Our team brings expertise from critical sectors where operational continuity is paramount. Crisis-proven and battle tested, we help agricultural technology providers protect innovations, secure supply chains, and maintain resilience across distributed operations.

Our services include risk-based vulnerability management, co-managed security programs, and cyber risk mitigation tailored to the IT/OT intersection that defines modern agriculture. We deliver practical, adaptive defenses that safeguard intellectual property and ensure business continuity without disrupting seasonal operations.

We combine strategic guidance with hands-on implementation to help agritech organizations build secure, agile infrastructures that protect critical data and meet regulatory obligations.

Executive Summary

The agritech sector is under sustained and intensifying attack. This is not a prediction. It is happening now, across Canada and the United States, at scale.

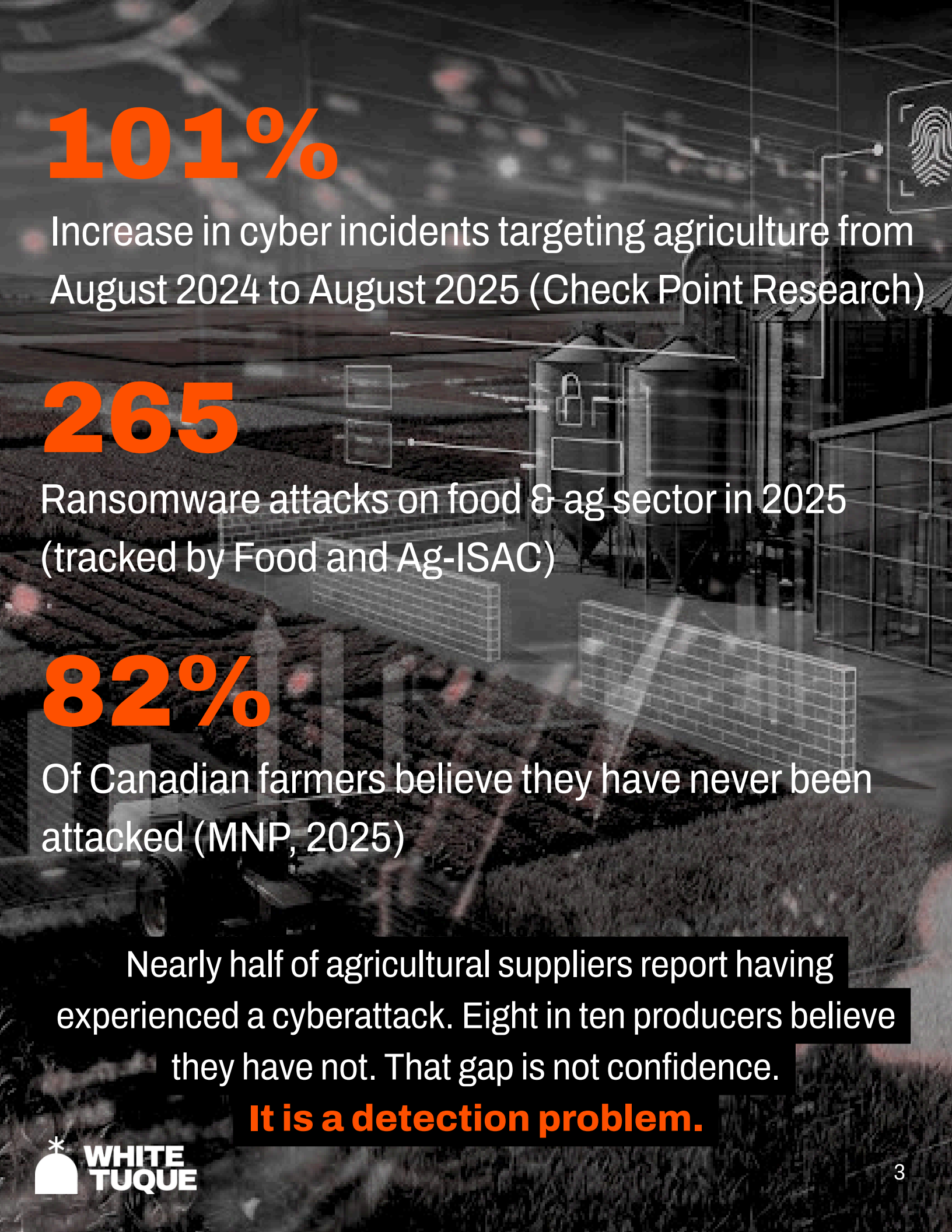
Ransomware attacks on food and agriculture operations rose 26 percent year over year in 2024 and nearly doubled again in early 2025. In October 2025, Canadian authorities confirmed that hacktivists had successfully tampered with operational technology systems at a grain drying facility, an oil and gas company, and a municipal water treatment plant, all within the same campaign window. The Canadian Centre for Cyber Security issued formal advisories. The grain silo attack, in which attackers remotely altered temperature and humidity readings, was a direct manipulation of the physical conditions that determine whether stored product is safe or spoiled.

This is not an IT problem. It is an operations problem. And it lands on your desk.

This brief is written for the person responsible for keeping the operation running, not the person responsible for the network. If you manage production schedules, vendor relationships, facility systems, or supply chain continuity, the risks described here are yours to manage, whether or not you have a dedicated security team.

This brief covers four areas:

- What drives the increase in attacks on agritech
- Where the real exposure sits in a modern agricultural operation
- What an attack actually looks like from an operations perspective
- What it takes to get ahead of it



101%

Increase in cyber incidents targeting agriculture from August 2024 to August 2025 (Check Point Research)

265

Ransomware attacks on food & ag sector in 2025 (tracked by Food and Ag-ISAC)

82%

Of Canadian farmers believe they have never been attacked (MNP, 2025)

Nearly half of agricultural suppliers report having experienced a cyberattack. Eight in ten producers believe they have not. That gap is not confidence.

It is a detection problem.

WHITE TUQUE

01. Why Agritech Is A Priority Target

The sector was not always high on the threat landscape. For most of cybersecurity's modern history, agritech was an afterthought. That changed when agritech stopped being analog.

Today, a mid-sized growing operation runs irrigation automation, climate control systems, nutrient dosing equipment, GPS-guided field machinery, and cloud-based crop management platforms. A food processor ties together ERP systems, cold chain monitoring, logistics platforms, and packaging line PLCs. A cannabis LP submits monthly regulatory reports to Health Canada, maintains electronic patient records, and tracks every gram through a federal chain of custody system. These are not isolated tools. They are interconnected, and they reach the internet.

Threat actors go where the leverage is. In agritech, the leverage is time. You cannot pause a harvest. You cannot hold a cultivation cycle while you negotiate with a ransomware group. A processing plant that goes down during a contracted delivery window does not get a grace period from its customers. This time pressure is exactly what criminal groups exploit, and they have noticed that the agricultural sector has historically underinvested in defenses.

In October 2025, Canadian hacktivists accessed a grain drying silo's control system and altered temperature and humidity readings. No custom malware, no sophisticated intrusion. They found an internet-connected system with a weak password and walked in. The Canadian Centre for Cyber Security issued a formal advisory.

(Source: Canadian Centre for Cyber Security, October 2025)

01. Why Agritech Is A Priority Target

The Numbers Behind the Trend

Check Point Research reported a 101 percent increase in cyberattacks targeting the agriculture sector between August 2024 and August 2025, the largest single-year sector increase they tracked across any industry. The Food and Agriculture Information Sharing and Analysis Center recorded 265 ransomware incidents against the sector in 2025, up from 212 in 2024 and 167 in 2023. The direction is consistent and the acceleration is steepening.

The Canadian Centre for Cyber Security's 2025-2026 National Cyber Threat Assessment confirmed that the frequency and severity of incidents against Canadian operations have both increased sharply, with essential services providers among the most affected. The Cyber Centre also flagged AI-assisted social engineering as an escalating vector, lowering the technical bar for attackers while making phishing and impersonation attacks harder to detect.

In Q1 2025 alone, Food and Ag-ISAC tracked 84 ransomware incidents against the sector, roughly one every two days.

Who Is Behind It?

Most attacks on agritech operations are not sophisticated nation-state campaigns. They are carried out by organized criminal groups using ransomware-as-a-service platforms, meaning criminal entrepreneurs buy access to proven malware toolkits and deploy them against targets of opportunity.

The dominant groups active in food and agriculture in 2025 include Qilin, which led sector targeting with 16 percent of tracked attacks, RansomHub, Akira, and Clop. These are not groups that specifically hate agriculture. They target sectors where operations cannot afford downtime, where security maturity tends to be lower than in finance or healthcare, and where payment history is consistent. Agritech checks all three.

Hacktivists represent a smaller but distinct threat category. The October 2025 Canadian campaign, which targeted the grain facility, was hacktivist in motivation: the goal was disruption and public attention, not financial gain. The attackers did not use sophisticated tools. They found internet-exposed control systems with weak or default passwords and changed parameters through the front door. That is a deterrent problem, not a sophisticated intrusion.

02. Where the Exposure Actually Lives

Most conversations about agricultural cybersecurity focus on office computers and email. Those are the wrong places to look first. The real exposure in a modern agritech operation sits in the systems that run the physical environment.

This is what makes agritech different from most industries: a successful attack can affect living things. Temperature controls that fail in a cannabis facility affect the crop. Humidity manipulation in a grain silo affects the safety of stored product. A compromised cold chain monitoring system for a food processor affects whether product reaches market safely. These are not data loss events. They are operational failures with physical consequences.

Operational Technology: The Forgotten Attack Surface

Operational technology, or OT, refers to the hardware and software that controls physical processes. In agriculture, this includes climate control systems, irrigation automation, SCADA systems managing multiple site functions, PLCs running processing line equipment, and the sensors feeding all of them data. These systems were designed for reliability and longevity, not security. Many are running software that has not been patched in years, some that cannot be patched without breaking the process it controls.

The problem compounds when OT systems are connected to business networks without proper segmentation. In many operations, the system managing your climate controls shares a network with the laptop your office manager uses to handle payroll. That is not a hypothetical. It is common. And it means that a phishing email opened in the office can, in the right circumstances, become a pathway to your production environment.

The October 2025 grain silo attacks exploited exactly this. The compromised systems were internet-exposed without adequate access controls.The attackers did not need to defeat sophisticated defenses. They needed an exposed interface and a weak credential.

02. Where the Exposure Actually Lives

Supply Chain: The Entry Point You Do Not Control

Modern agritech operations do not operate in isolation. You have equipment vendors with remote access to diagnostic systems. You have logistics partners connected to your tracking platforms. You have SaaS providers hosting your farm management software. You have co-packers with visibility into your production schedules. Each of these is a potential entry point into your environment, and each one has its own security posture that you likely cannot assess and certainly cannot control.

This is the supply chain risk that keeps operations leaders up at night, because the exposure is structural. You are not going to stop working with vendors. The question is whether you have visibility into what those relationships look like from an attacker's perspective, and whether you have contractual and technical controls in place to limit what a compromised vendor can reach inside your systems.

The Food and Ag-ISAC notes explicitly that the sector's interconnected supply chains mean a disruption at one node can cascade across the entire chain. Just-in-time delivery models amplify this: there is no buffer to absorb a delay caused by a vendor incident.

02. Where the Exposure Actually Lives

The Regulatory Dimension

Canadian agritech operations are subject to PIPEDA, which governs the handling of personal information across federally regulated activities, including medical patient records held by licensed cannabis producers. Health Canada's Cannabis Tracking and Licensing System requires monthly electronic reporting; a breach that compromises those systems or their data integrity puts your licence itself at risk, not just your data.

The federal government reintroduced its critical infrastructure cybersecurity legislation as Bill C-8 in June 2025, following the death of its predecessor Bill C-26 when Parliament was prorogued in January 2025. As of early 2026, Bill C-8 is progressing through committee. When it passes, it will establish mandatory cybersecurity programs, 72-hour incident reporting obligations, and supply chain oversight requirements for designated operators. Agriculture is not yet formally designated as critical infrastructure under the bill, but the Centre for International Governance Innovation and other policy bodies have argued it should be, and the regulatory direction is clear.

In the U.S., CISA's food and agriculture critical infrastructure designation and the Farm and Food Cybersecurity Act currently before Congress are moving the sector toward enforceable standards. Operators with U.S. distribution partners or customers are already feeling this pressure through supply chain security requirements.

80% of Canadian farmers believe they have never experienced a cyberattack. Nearly half of their suppliers report that they have.
That is not a security posture.
That is a visibility problem.

(Source: MNP Digital, Cyber Security on the Farm 2025 Report)

03. What an Attack Looks Like from the Operations Side

Security briefings tend to describe attacks in technical terms. This one will not. Here is what a ransomware incident looks like when you are the person managing the operation.

You arrive on a Monday morning, and your production management system is not responding. Your team cannot access the scheduling platform. Someone has already called the ERP vendor. The IT contact, if you have a dedicated one, is on the phone. Nobody is certain yet what happened. The message, when it arrives, is usually straightforward: your files have been encrypted, and here is a Bitcoin address.

What happens next depends entirely on what you built before that Monday morning.

If you have tested backups that are isolated from your production network, you have options. If your backups are on the same network that got encrypted, they are also encrypted. If you have an incident response plan with clear decision authority, your leadership team knows within the first hour who is making decisions, what gets communicated to customers, and when to involve law enforcement. If you do not, you will spend the first 48 hours doing that work under pressure, while a clock is running.

The operational consequences compound fast. A processing facility that cannot access its ERP will miss delivery windows. Missed delivery windows trigger contractual penalties and customer escalations. A cultivation facility that loses climate control visibility, even temporarily, faces crop risk. A cannabis LP that cannot submit its monthly CTLS report faces regulatory scrutiny.

03. What an Attack Looks Like from the Operations Side

The Attack Progression That Operations Leaders Need to Understand

Most ransomware attacks do not begin with encryption. They begin with access, often weeks or months before anything visible happens. The attacker gains a foothold, typically through a phishing email or an exposed remote access system, and then moves quietly through the environment, mapping what is there, identifying where the backups are, and establishing persistence. The encryption is the last step, not the first.

According to Food and Ag-ISAC reporting, approximately 83 percent of attacks on agritech operations involve targeted spishing (spear phishing) attacks as the initial access vector. That means someone in your organization received an email and clicked something. It is not a failure of intelligence. It is a numbers game, and the attackers are patient.

The implication for operations leaders is this: by the time you know you have been hit, the attacker has likely been in your environment for a while. The question is not just how you respond to the encryption event. It is whether you have detection capability that would have caught the attacker during the reconnaissance and lateral movement phase, before the payload deployed.

The Specific Risk Profile of Agritech

Three factors make agritech a particularly high-consequence environment for a ransomware incident, compared to most other industries:

1. Biological time pressure. A harvest window is measured in days. A cultivation cycle cannot be paused. A perishable goods processing line running behind creates waste, not just delay. This is the pressure point attackers exploit, and it is one that most other industries do not face in the same form.

2. Physical consequence potential. Beyond financial and reputational damage, attacks on OT systems in agriculture carry the risk of physical harm: compromised cold chain integrity, tampered environmental controls, or manipulated sensor data that leads to decisions made on false information. The October 2025 grain silo incident demonstrated that this is not theoretical.

3. Regulatory exposure on multiple fronts. A breach affecting medical patient data held by a licensed cannabis producer, or compromising the integrity of CTLS reporting, carries consequences that go beyond damage control. It can affect licence status.

04. What Getting Ahead of It Actually Looks Like

Cybersecurity in agritech does not require a large IT department or an enterprise security budget. It requires clarity about what you are protecting, where the real exposure is, and what you would do if something went wrong.

Most agritech operations that have been through a serious incident report the same thing afterward: the gaps were knowable. The exposed systems, the weak credentials, the backup that had not been tested, the vendor with broader access than they needed. None of it required sophisticated analysis to identify. It required someone to look.

Start with Visibility

You cannot protect what you cannot see. The first step for most operations is a clear picture of what is connected to what: which systems have internet exposure, which vendor relationships involve remote access, where your OT environment touches your business network, and where your backups actually live.

This is not a technical audit in the conventional sense. It is an operational inventory. And it is the foundation of everything else, because the risk decisions you make after this step depend entirely on having accurate information about your environment. Most operations are surprised by what this brings to the surface.

04. What Getting Ahead of It Actually Looks Like

Separate Your Operating Environment

The single most impactful structural change that most agritech operations can make is network segmentation: keeping the systems that control physical processes on a separate network from the systems used for business operations, administration, and internet access. This does not eliminate risk, but it breaks the most common attack path, which runs from a phishing email in the office to lateral movement into the OT environment.

This is an investment, and it requires proper planning to implement without disrupting operations. But it is the structural change that most meaningfully reduces your exposure to the category of attack that is actually targeting your sector.

Know What Your Vendors Can Touch

Remote access by third-party vendors is one of the most consistently exploited entry points in OT environments across all sectors. The equipment OEM that has ongoing remote diagnostic access to your processing line, the logistics partner with API access to your inventory system, the SaaS provider whose platform has read access to your crop management data: each of these relationships needs to be inventoried and assessed.

The practical questions are straightforward:
What access does each vendor have?
Is it always-on or session-based? Is it logged?
When was it last reviewed?

Most organizations find, when they look, that vendor access has expanded over time and has not been cleaned up as relationships have evolved.

04. What Getting Ahead of It Actually Looks Like

Test Your Recovery Before You Need It

The most common discovery after a ransomware incident is that the backup did not work the way the operations team thought it did. Either it was on the same network and got encrypted, or it had not been tested and the restoration process failed, or the recovery time was much longer than expected because nobody had actually run through it.

Incident response is a skill that degrades without practice. A tabletop exercise, which is essentially a structured walkthrough of what your team does in the first 24 and 72 hours of a serious incident, identifies these gaps before they matter. It also clarifies the decision authority questions that tend to paralyze organizations under pressure:

Who has the authority to take systems offline?
Who communicates with customers?
Who makes the call on whether to engage law enforcement?

This does not require significant technical infrastructure. It requires an afternoon, the right people in the room, and a facilitator who knows what questions to ask.

The Role of External Expertise

Most agritech operations do not have, and do not need, a full-time Chief Information Security Officer. What they need is access to senior security expertise on a periodic basis: to assess posture, to advise on the right priorities, to run the tabletop exercise, to be on the phone in the first hours of a serious incident. Fractional security leadership, structured properly, gives you that access without the overhead.

The key word is senior. The analysis of where you are exposed and what you should do about it requires experience with the kinds of attacks that are actually targeting your environment. Generic cybersecurity advice is abundant and largely useless. What matters is someone who has been inside enough incidents to know what the threat actors actually do, how they move, and where operations like yours tend to get caught.

A Practical Approach to Protection

Incident response is a skill. It degrades without practice. The organizations that come through serious incidents with the least damage are not the ones with the biggest budgets.

They are the ones that planned ahead.

The Bottom Line

The threat to agritech is real, it is current, and it is increasing. The organizations that navigate it best are not the ones that assume they are too small to be targeted or too complex to be understood. They are the ones that looked honestly at where they were exposed and took practical steps to reduce it.

The good news is that the most impactful steps are not technically sophisticated. Visibility, segmentation, vendor access control, and tested recovery: these are fundamentally operational disciplines, not IT projects. The operations leader is not the wrong person to own this. In many respects, they are the right person.

White Tuque works with agritech operations to build security programs that fit how your business operates. We start with understanding your environment, not applying an all-purpose framework. We work directly with your team, and we deliver recommendations your organization can action, not a generic compliance report that sits in a drawer.

If you want a clear picture of where your operation stands, that conversation starts with a risk assessment.

Sources referenced in this brief:

Check Point Research, Global Cyber Threats Report August 2025
Food and Agriculture ISAC, 2025 Ransomware Landscape Report (February 2026)
Canadian Centre for Cyber Security, Advisory on Hacktivist ICS Attacks, October 2025
Canadian Centre for Cyber Security, National Cyber Threat Assessment 2025-2026
MNP Digital, Cyber Security on the Farm 2025 Report
RSM Canada, Ransomware Pressure Rises for Food and Agriculture Businesses (March 2026)
SecurityBrief Canada, From Bill C-26 to C-8: Canada's Cyber Law Reboot Explained (March 2026)
TechRepublic, Canada Warns of Cyberattacks Targeting Industrial Control Systems (October 2025)
Association of Equipment Manufacturers, Cyber Threats Are the New Pest in Agriculture (2025)
Centre for International Governance Innovation, Canada's Draft Cybersecurity Legislation Must Be Resurrected (April 2025)