VIEW POINT



# CYBER HARVEST - WHY FOOD SECURITY IS BECOMING THE NEXT CYBERSECURITY BATTLEGROUND

## A POINT OF VIEW ON THE GROWING CYBER THREAT TO AGRICULTURE AND FOOD PRODUCTION


### Abstract

For generations, agriculture has been shaped by risks that are largely visible and tangible: extreme weather, disease outbreaks, labour shortages, fuel costs, supply chain bottlenecks, and market volatility. Today, however, an invisible threat is rapidly emerging, one capable of disrupting food production at scale without a single physical intrusion.

Cybersecurity is no longer an issue confined to corporate offices and financial institutions. As farming becomes increasingly digitised and connected, cyber threats are beginning to challenge the resilience of agricultural operations, food supply chains, and ultimately national food security itself.


Infosys
Navigate your next

# Introduction

The modern farm is evolving into a complex digital ecosystem. Grain dryers can be monitored remotely through mobile devices. Precision agriculture platforms analyse field conditions in real time. Livestock welfare systems automatically adjust feeding, ventilation and environmental controls. Irrigation systems respond dynamically to weather forecasts. Farm management software tracks everything from crop yields and regulatory reporting to financial performance and commodity sales. To removing minimal waste from grading lines and sorting categorisation of crops to table.

This digital transformation is delivering enormous productivity benefits. At the same time, it is creating a new dependency that many agricultural businesses may underestimate. When Operational Technology (OT) becomes dependent on connectivity, cyber resilience becomes inseparable from operational resilience.

The agricultural sector now faces cybersecurity challenges remarkably like those encountered by the energy, water and transportation sectors in the past decade. Yet unlike these industries, farming has historically not been viewed as critical infrastructure worthy of significant cyber investment. Threat actors increasingly recognise this reality. Disrupting the raw materials of the food chain can disrupt the entire food chain and affect end recipients.

## From Opportunistic Crime to Strategic Disruption

Historically, most farms viewed cybercrime primarily as an issue of financial fraud, the stealing of physical OT items from their tractors or stolen credentials that remotely operate machinery. While these threats remain significant, the threat landscape is changing.

Sophisticated attackers are increasingly focused on disruption rather than simply theft.

Imagine a harvest period where dozens of grain dryers across multiple counties begin behaving erratically. Moisture settings change unexpectedly. Temperature controls fluctuate. Automated shutdown mechanisms could be triggered repeatedly, while a compromised grading machine may fail to remove poor-quality produce, allowing defective crops to be mixed with healthy ones. This could degrade the quality of the overall harvest, potentially resulting in significant crop losses.

Operators lose visibility and confidence in their systems at precisely the moment they are needed most.

This scenario is not theoretical. Even recent incidents have demonstrated how connected agricultural equipment can become vulnerable when exposed to remote access and internet connectivity.

In the future, state-sponsored attack scenarios, such as the incidents mentioned above, may no longer occur in isolation as they have in the past, but instead may be coordinated and executed collectively to disrupt critical national infrastructure, including the farming and food supply chain. Attackers could exploit vulnerabilities across software suppliers, machinery manufacturers, logistics providers, and agricultural service firms, triggering disruption throughout the broader agricultural ecosystem rather than targeting a single farm or production process. The impact could cascade across a wide network of interconnected supporting functions, with the attackers' objectives extending beyond financial gain to broader economic, societal, or geopolitical disruption. Instead, to create uncertainty, operational disruption and economic consequences throughout the food production chain and across a country or region.



External Document © 2026 Infosys Limited

# The Emerging Risk of Data Integrity Attacks

Many discussions around cybersecurity focus on ransomware and system availability. However, one of the most concerning future threats to agriculture may involve the manipulation of 'data' rather than the destruction of it. Modern agricultural decisions increasingly depend upon digital information. Farmers rely on yield forecasts, soil analytics, irrigation recommendations, livestock health indicators, progressive cropping, commodity inventory data and environmental monitoring platforms. If the attackers manipulate these data sources, operational decisions may be compromised long before anyone realises a cyber incident has occurred.

A manipulated irrigation system or recommendation could damage crops through overwatering, potentially spoiling them before they are fully established or even partially established. Altered grain moisture readings could reduce storage quality. Spraying levels adjusted upwards or downwards to ruin crops and incorrect livestock monitoring data could affect welfare outcomes. False inventory levels could create disruption throughout food processing and distribution networks.

This mirrors the strategic thinking behind sophisticated industrial attacks such as Stuxnet, where manipulated operational data concealed ongoing disruption. In the future, the most dangerous agricultural cyberattack may not be immediately visible. It may quietly convince operators that everything is functioning normally while business performance steadily deteriorates.

The most dangerous agricultural cyberattack may not stop operations. It may quietly manipulate trusted data and drive the wrong operational decisions.



**HIDDEN MANIPULATION**

**TRUSTED DIGITAL DATA**
Yield, soil, irrigation, livestock, inventory and environmental data

**DATA IS ALTERED**
Plausible values conceal unreliable readings and recommendations

**FALSE DECISIONS**
Operators act on incorrect settings, forecasts, readings or stock levels

**DAMAGE EMERGES**
Performance and quality deteriorate before the incident is recognised

**Systems appear normal while operational outcomes steadily worsen**



**IRRIGATION**
Manipulated recommendations can drive overwatering, crop damage or failure during establishment.



**GRAIN STORAGE**
Altered moisture readings can reduce storage quality and conceal deterioration.



**SPRAYING LEVELS**
Upward or downward adjustment can damage crops, reduce yield or ruin production.



**LIVESTOCK WELFARE**
Incorrect monitoring data can delay intervention and compromise welfare outcomes.



**INVENTORY & DISTRIBUTION**
False stock levels can disrupt processing, fulfilment and food distribution networks.

KEY RISK: Operators continue to trust manipulated data and apparently normal system behaviour.

Cyber resilience must protect availability and the accuracy, provenance and trustworthiness of operational data.

*Fig. The Emerging Risk of Data Integrity Attacks*



External Document © 2026 Infosys Limited

# Artificial Intelligence is Changing the Game

The emergence of artificial intelligence is accelerating this threat landscape.

In the past, launching a sophisticated cyberattack demanded significant technical expertise. Today, AI-powered tools are lowering barriers to entry and allowing attackers to operate at unprecedented scale.

Phishing emails can now be personalised using publicly available information and crafted in flawless English. Voice-cloning technologies can impersonate trusted suppliers, grain merchants or family members. Automated reconnaissance tools can identify vulnerable systems within minutes. Malware can adapt dynamically to evade traditional security controls.

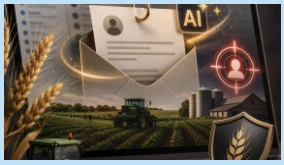
For agricultural businesses, many of which operate with lean resources and limited technology teams, this represents a significant challenge. Threat actors are becoming more capable while defenders often remain constrained by time, budget and specialist expertise.

AI is lowering barriers to entry, increasing attack scale and accelerating the speed at which agricultural businesses can be targeted.

**PAST ATTACK MODEL**
High technical expertise • slower preparation • limited scale

**AI ACCELERATION**
Automation | Personalisation | Adaptation

**CURRENT THREAT MODEL**
Lower entry barriers • rapid targeting • unprecedented operating scale




**AI-PERSONALISED PHISHING**

Public information can be used to create convincing, targeted messages in polished language.



**VOICE CLONING**

Trusted suppliers, grain merchants or family contacts can be convincingly impersonated.



**AUTOMATED RECONNAISSANCE**

Connected farm systems and vulnerable services can be identified within minutes.



**ADAPTIVE MALWARE**

Malware can change behaviour dynamically to evade traditional security controls.



**THE CAPABILITY IMBALANCE**

Threat actors become more capable while agricultural defenders remain constrained

Lean resources | Limited technology teams | Time, budget and specialist expertise constraints

The strategic question is no longer whether attackers can use AI. It is how agricultural businesses build proportionate resilience against AI-enabled scale and speed.

*Fig. Artificial Intelligence is Changing the Game*



External Document © 2026 Infosys Limited

# Why Agriculture Must Think Differently About Cybersecurity

One of the greatest misconceptions within agriculture is that businesses are too small or too specialised to attract sophisticated adversaries.

Attackers often seek the path of least resistance. Agriculture presents a highly attractive target because operational downtime has immediate consequences. Harvest cannot wait. Livestock cannot pause. Food distribution cannot simply stop until systems are restored. This creates pressure that attackers understand and exploit.

As a result, cybersecurity within the agricultural sector must evolve beyond traditional IT thinking. The conversation should no longer focus solely on computers, software and passwords. Instead, it should focus on operational continuity and business resilience.

The fundamental question is not how to prevent every attack. No industry has achieved that goal. The real question is whether farming operations can continue if critical systems become unavailable.

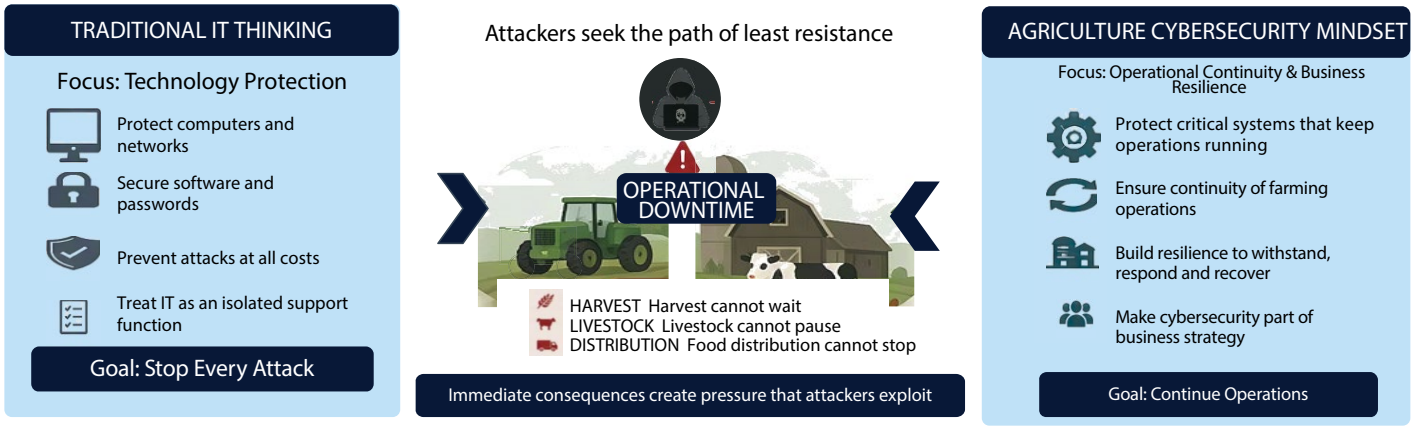



*Fig. Why Agriculture Must Think Differently About Cybersecurity*

# Building a Cyber-Resilient Farming Sector

A resilient agricultural enterprise begins with recognising that cyber risk is now a business risk.

The most successful farming businesses increasingly view grain dryers, livestock management systems, irrigation controls and precision farming technologies as critical operational assets requiring the same protection as physical machinery and infrastructure.

This means securing remote access capabilities, ensuring operational technology is separated from general office networks, and maintaining oversight of all connected equipment deployed across the farm.

Equally important is the protection of agricultural data. Many farming businesses depend heavily on digital records accumulated over decades, yet these assets are often inadequately protected. Yield analysis, crop histories, stewardship records and financial forecasts may ultimately prove as valuable to a modern farming enterprise as any physical asset. Robust backup arrangements, offline recovery capabilities and tested restoration procedures therefore become essential components of resilience.

The human element remains another critical factor. Most successful cyber intrusions continue to originate through phishing emails, social engineering or compromised credentials. As attackers increasingly leverage artificial intelligence to create highly convincing messages, awareness and training become some of the most effective security investments available. Cybersecurity awareness must become as ingrained within farm operations as health and safety practices have become over previous decades.

External Document © 2026 Infosys Limited

As farming becomes digitised and connected, cyber threats can challenge agricultural operations, food supply chains and national food security.



THE MODERN CONNECTED FARM

Remote grain drying | Precision agriculture | Livestock controls | Dynamic irrigation | Yield & compliance | Commodity sales | Grading & waste reduction

**CONNECTIVITY CREATES DEPENDENCY**



When Operational Technology depends on networks, cloud platforms, mobile access and data, cyber disruption becomes operational disruption.



**FOOD PROCESSING & SUPPLY CHAIN**

Operational dependencies extend beyond the farm gate.



**NATIONAL FOOD SECURITY**

Resilience of connected farming contributes to continuity of food supply.

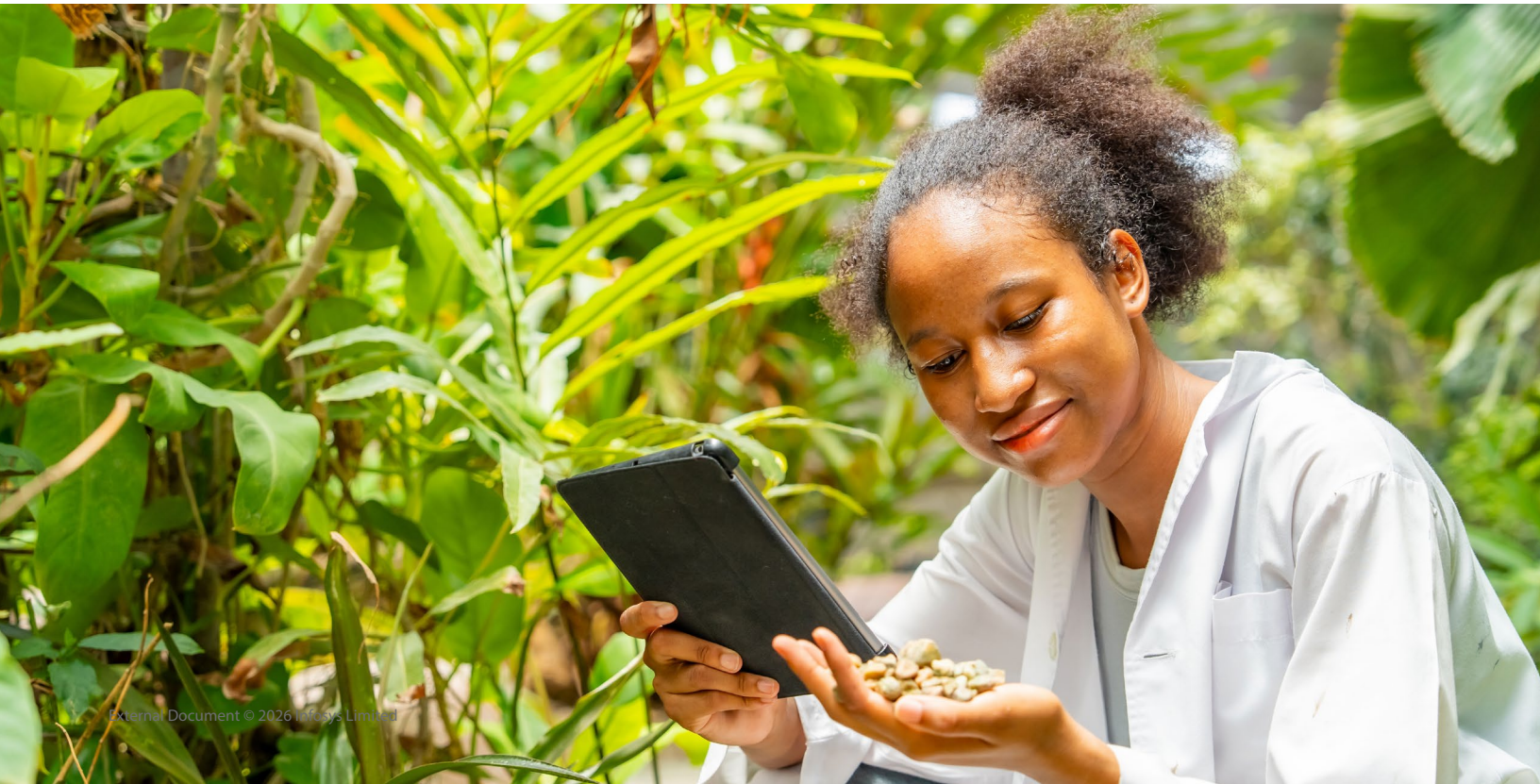
DIGITAL TRANSFORMATION + CONNECTIVITY & DEPENDENCY = CYBER RESILIENCE IS OPERATIONAL RESILIENCE

The risk is not simply the equipment. The risk is the connectivity and data on which modern agricultural operations increasingly depend.

*Fig. Cybersecurity is Now a Food Security Issue*

Supply chain security will also become increasingly important. Farmers now depend on a broad ecosystem of machinery manufacturers, software providers, grain merchants, contractors and logistics partners. A compromise within a single supplier may ultimately affect hundreds or thousands of customers. Increasingly, resilience will require confidence not only in one's own cybersecurity posture but also in that of key partners and service providers.

Finally, the agricultural sector must embrace the concept of operational resilience. Every farm should have a practical understanding of how critical activities would continue during a prolonged technology outage. Whether driven by ransomware, supply chain compromise or infrastructure disruption, the ability to operate manually for a defined period may become one of the most important resilience capabilities a farming business can possess.



External Document © 2026 Infosys Limited

Digital farming improves productivity and sustainability, but cyber disruption can directly affect operations, animal welfare, supply-chain continuity and confidence in food production.

### AGRICULTURAL CYBER RISK LANDSCAPE

**!** **Ransomware & OT Outages**
Loss of grain drying, irrigation, livestock, processing or distribution capability.

**D** **Data Integrity Attacks**
Manipulated readings or forecasts can drive harmful operational decisions.

**AI** **AI-Enabled Attacks**
Personalised phishing, voice cloning, automated targeting and adaptive malware.

**S** **Supply-Chain Compromise**
Vendors, service providers, machinery platforms and logistics partners can introduce risk.

**IoT** **Connected Equipment & IoT**
Tractors, sensors, drones, weather stations and smart controls expand the attack surface.

**C** **Cloud & Farm Platforms**
Loss of access can affect operational records, compliance data and business systems.

**H** **Human Error & Insider Risk**
Credential compromise, misconfiguration or unauthorised access can initiate disruption.

**£** **Fraud & Impersonation**
Business email compromise can redirect payments, goods or commodity transactions.

### WHAT IS AT STAKE?

| | |
|---|---|
| **CROP PRODUCTION** | Yield, quality and seasonal timing |
| **LIVESTOCK WELFARE** | Feeding, ventilation and monitoring |
| **WATER & ENVIRONMENT** | Irrigation and environmental controls |
| **STORAGE & PROCESSING** | Grain quality, grading and handling |
| **CONNECTED EQUIPMENT** | Machinery, sensors and automation |
| **FOOD SUPPLY CHAINS** | Processing, transport and distribution |
| **NATIONAL FOOD SECURITY** | Continuity and trust in food production |

**THE GREATEST RISK IS NOT SIMPLY LOSS OF DATA** — It is the loss of operational capability, supply-chain continuity and trust in the systems supporting modern food production.

**Cybersecurity protects more than computers. It protects the continuity, safety and resilience of modern agriculture.**

*Fig. Key Cyber Risks in Agriculture Sector*

# Conclusion: Food Security is National Security

Over the next decade, the agricultural sector will continue its transition towards automation, connectivity and data-driven decision making. This transformation will deliver significant gains in productivity, sustainability and efficiency. However, it will also create new dependencies and vulnerabilities.

Just as energy, water and transportation systems are now recognised as critical national infrastructure, food production must increasingly be viewed through the same lens.

The next agricultural crisis may not begin with drought, disease or market instability. It may begin with a compromised supplier, an AI-generated phishing email, a manipulated sensor reading or a malicious software update delivered silently through a trusted partner.

The future of farming will undoubtedly be digital. Ensuring it is also secure will be essential to protecting not only individual farms and agribusinesses, but the resilience of national food systems themselves.

The future battlefield for food security is no longer confined to the field, the farm or the distribution centre. It extends into every network, every connected device and every digital decision supporting modern agriculture.



External Document © 2026 Infosys Limited

# About the Author



**Luke Smith**

*AVP – Senior Practice Engagement Manager*

Luke is an accomplished cybersecurity leader with deep experience in building and strengthening enterprise security programs. He specializes in protecting critical data assets, enhancing security resilience, and supporting compliance initiatives. With expertise spanning cybersecurity frameworks, cloud environments, and infrastructure security, Luke helps organizations address complex security challenges and achieve their strategic objectives.

For more information, contact askus@infosys.com

Infosys®
Navigate your next

© 2026 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.