



Shutterstock: Fotokostic

Sep 05, 2019 22:06 BST

## Staying secure in a changing agricultural landscape

**Agriculture is essential for modern society. Arguably, it has never been more important – with climate change, population growth, demographic changes, and water scarcity, it's vital that the food industry adapts and adopts technology to meet the growing demands on the food supply chain and network.**

The UK's agriculture industry has changed dramatically in recent years. Farms have increasingly adopted emerging technologies as a way to improve efficiency and cut down on costs, and terms such as 'smart farming' and

'precision farming' have come into popular use.

However, with the increasing adoption of digital technologies comes a growing cyber security threat. While this is true for all industries, the agriculture sector faces its own unique challenges.

For example, concerns around animal welfare mean that agriculture organisations can face threats from hacktivists wishing to cause financial damage. As well as this, the UK's food sector is classed as critical national infrastructure, which makes it a potential target for nation-state actors.

Having effective cyber security measures in place is crucial if organisations want to implement and maintain effective digital processes. Many of the individual businesses that make up the UK's agriculture sector are small or micro-enterprises, which are less likely to have strong defences in place. Additionally, complex supply chains and a reliance on third-party infrastructure can make it difficult to quantify cyber risk, which is where government departments and security specialists can step in to help to improve knowledge and share best practice.

Large food processors can also face cyber security threats and be targeted by activists and sophisticated nation-state actors that want to cause disruption to a supply chain. Although food shortages would be unlikely, a successful attack on just one of these large organisations could affect a large number of farmers and growers.

It's important to understand the potential risks that can arise from the UK's complex and interconnected food network. From databases containing confidential and often critical data about farm produce and livestock, to internet-connected vehicles and heating, ventilation and air conditioning (HVAC) systems in storage spaces, increasing digitisation can present a vast attack surface.

Along with Harper Adams University, our research team has been working on an in-depth analysis of the UK's agriculture sector, exploring potential risks and outlining how industry and government can work together to improve the resilience of the nation's food network.

Download our whitepaper from the link below

---

## About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

## Contacts



### **NCC Group Press Office**

Press Contact

All media enquires relating to NCC Group plc

[press@nccgroup.com](mailto:press@nccgroup.com)

+44 7824 412 405

+44 7976 234 970



### **NCC Group - Financial Media Enquiries**

Press Contact

Maitland AMO

Financial Results Media Enquiries

+44 (0)20 7379 5151



## **Regional Press Office - North America**

Press Contact

[NCCGroup@cdc.agency](mailto:NCCGroup@cdc.agency)

+1 408 776 1400

+1 408 893 8750