For more insight into our expertise and services

# Agriculture, Aquaculture & Fishing

1 July 2026

SOUTH AFRICA

- From field to firewall: Why cybersecurity is the new frontier for agricultural businesses

SOUTH AFRICA

# From field to firewall: Why cybersecurity is the new frontier for agricultural businesses

Agricultural businesses have increasingly adopted technology across their operations – from precision farming tools and automated machinery to artificial intelligence-driven (AI-driven) analytics and IoT-enabled sensors – to monitor soil conditions, precipitation levels, livestock health and crop yields. While these advancements have enhanced productivity and enabled data-driven decision-making, they have simultaneously exposed agricultural businesses to a growing array of cybersecurity threats.

AgriTech adoption has increased significantly as businesses seek to improve productivity, decrease wastage and address labour shortages. AgriTech and the addition of AI machine learning can be used to analyse data from sensors, drones and weather stations to provide real-time recommendations on irrigation, fertilisation, crop rotation and pest management, which optimises crop yields and livestock health. However, with this increased reliance on technology comes a corresponding increase in the attack surface available to threat actors seeking to exploit vulnerabilities in AgriTech systems.

The more integral technology is in day-to-day agricultural practices, the greater the impact of a cybersecurity incident. Common cybersecurity risks include:

- ransomware attacks where a threat actor encrypts a business's systems and demands payment for decryption keys;
- malware which damages, disrupts or allows a threat actor unauthorised access to the systems;
- zero-day exploits where a threat actor takes advantage of previously unknown vulnerabilities in the IT systems;
- distributed denial of service attacks where the threat actor overwhelms system capacity, making services unavailable to users;
- phishing and business email compromise where attackers manipulate individuals into divulging sensitive information;
- data breaches involving unauthorised access to, disclosure of, or theft of sensitive or confidential information; and
- supply chain attacks where a trusted third-party supplier or service provider is compromised and used to gain access to another business's systems.

# Agriculture, Aquaculture & Fishing

SOUTH AFRICA

There are already numerous examples of ransomware and other cyberattacks adversely affecting the agricultural food chain. They have disrupted crop production, livestock farming, meat processing, distribution and logistics.

The consequences of a cybersecurity incident can be severe. Ransomware locking operators out of farm management systems during critical planting or harvesting periods could result in significant crop losses. These attacks can result in operational downtime, environmental damage, compromise in food safety standards, supply chain disruptions and other forms of financial loss. For example, a breach of automated irrigation or livestock monitoring systems could lead to animal welfare concerns or crop failure. The theft of sensitive commercial data – such as proprietary farming techniques or supplier information – could undermine a business's competitive position. Agricultural businesses may also face regulatory penalties, reputational damage and litigation arising from a failure to comply with applicable data protection legislation.

When a cybersecurity incident occurs, a co-ordinated 'war-room' response is essential to minimise the impact and resume operations as quickly as possible. The following steps should be taken:

1. Prompt notification of your cyber insurance provider.
2. Appoint external legal counsel to guide you through the process and ensure the steps taken are covered by legal professional privilege.
3. Engage cybersecurity specialists through external legal counsel to investigate the incident.
4. Preserve evidence and contain the breach.
5. Consult with your reaction team, cyber insurers, legal advisors and cybersecurity specialists before paying any ransom.
6. Obtain legal advice to reduce potential liability and penalties.
7. Assess your regulatory notification requirements.
8. Prepare internal and external communications.
9. Keep records of steps taken.
10. Review the incident and improve security.

Further guidance on the steps to take after a data breach is available here.

Agricultural businesses deploying AgriTech must adopt a proactive approach to managing cybersecurity risks. Key measures to build cyber resilience include:

- conduct regular cybersecurity risk assessments across all deployed technology systems;
- implement cybersecurity awareness training for all employees, including on phishing and social engineering;
- establish robust access controls, including multi-factor authentication, for critical systems and sensitive data;
- maintain regular, secure and off-site backups of all critical data and systems;
- develop and regularly test a cybersecurity incident response plan with clearly defined roles and escalation procedures;

# Agriculture, Aquaculture & Fishing

SOUTH AFRICA

- ensure all software, firmware and operating systems are kept up to date with the latest security patches;
- conduct due diligence on third-party suppliers and ensure appropriate contractual cybersecurity protections are in place;
- obtain appropriate cyber insurance coverage; and
- engage legal counsel to ensure compliance with data protection legislation and to establish a framework for incident response and regulatory notifications.

The introduction of AgriTech for the digitisation of agricultural processes presents both significant opportunities and considerable risks. While it has the potential to revolutionise farming operations, agricultural businesses must recognise that the adoption of technology without adequate cybersecurity measures exposes them to threats that could have devastating operational, financial, and legal consequences. Building cyber resilience is not a once-off exercise but requires ongoing commitment, regular review, and continuous improvement of security measures. By implementing robust mitigation measures, developing comprehensive incident response plans and fostering a culture of cybersecurity awareness, agricultural businesses can harness the benefits of technology while safeguarding their operations and data against the ever-evolving landscape of cyber threats.

**Tayyibah Suliman and Izabella Balkovic**


# OUR TEAM

For more information about our Agriculture, Aquaculture & Fishing sector and services in South Africa, Kenya and Namibia, please contact:


**André de Lange**
Sector Head:
Agriculture, Aquaculture & Fishing
Director: Corporate & Commercial
T +27 (0)21 405 6165
E andre.delange@cdhlegal.com



**Sammy Ndolo**
Managing Partner | Kenya
T +254 731 086 649
+254 204 409 918
+254 710 560 114
E sammy.ndolo@cdhlegal.com



**Patrick Kauta**
Managing Partner | Namibia
T +264 833 730 100
M +264 811 447 777
E patrick.kauta@cdhlegal.com



**Tessa Brewis**
Sector Head: Projects & Energy
Director: Banking, Finance & Projects
T +27 (0)21 481 6324
E tessa.brewis@cdhlegal.com



**Petr Erasmus**
Director:
Tax & Exchange Control
T +27 (0)11 562 1450
E petr.erasmus@cdhlegal.com



**Simóne Franks**
Director:
Real Estate Law & Conveyancing
T +27 (0)21 481 6464
E simone.franks@cdhlegal.com



**Allan Hannie**
Director:
Corporate & Commercial
T +27 (0)21 405 6010
E allan.hannie@cdhlegal.com



**Andries Le Grange**
Director:
Competition Law
T +27 (0)11 562 1092
E andries.legrange@cdhlegal.com



**Sentebale Makara**
Director:
Dispute Resolution
T +27 (0)11 562 1181
E sentebale.makara@cdhlegal.com



**Richard Marcus**
Director:
Dispute Resolution
T +27 (0)21 481 6396
E richard.marcus@cdhlegal.com



**Burton Meyer**
Director:
Dispute Resolution
T +27 (0)11 562 1056
E burton.meyer@cdhlegal.com



**Lucinde Rhoodie**
Director:
Dispute Resolution
T +27 (0)21 405 6080
E lucinde.rhoodie@cdhlegal.com



**James Ross**
Director:
Corporate & Commercial
T +27 (0)21 481 6424
E james.ross@cdhlegal.com



**Belinda Scriba**
Director:
Dispute Resolution
T +27 (0)21 405 6139
E belinda.scriba@cdhlegal.com



**Tayyibah Suliman**
Sector Head:
Technology & Communications
Director: Corporate & Commercial
T +27 (0)11 562 1667
E tayyibah.suliman@cdhlegal.com



**Alistair Young**
Director:
Corporate & Commercial
T +27 (0)11 562 1258
E alistair.young@cdhlegal.com



**Alecia Pienaar**
Counsel:
Environmental Law
M +27 (0)82 863 6279
E alecia.pienaar@cdhlegal.com



**Liëtte van Schalkwyk**
Senior Associate:
Dispute Resolution
T +27 (0)11 562 1686
E liette.vanschalkwyk@cdhlegal.com

**BBBEE STATUS:** LEVEL ONE CONTRIBUTOR
Our BBBEE verification is one of several components of our transformation strategy and we continue to seek ways of improving it in a meaningful manner.

**PLEASE NOTE**
This information is published for general information purposes and is not intended to constitute legal advice. Specialist legal advice should always be sought in relation to any particular situation. Cliffe Dekker Hofmeyr will accept no responsibility for any actions taken or not taken on the basis of this publication.

**JOHANNESBURG**
1 Protea Place, Sandton, Johannesburg, 2196. Private Bag X40, Benmore, 2010, South Africa.
Dx 154 Randburg and Dx 42 Johannesburg.
T +27 (0)11 562 1000 F +27 (0)11 562 1111 E jhb@cdhlegal.com

**CAPE TOWN**
11 Buitengracht Street, Cape Town, 8001. PO Box 695, Cape Town, 8000, South Africa. Dx 5 Cape Town.
T +27 (0)21 481 6300 F +27 (0)21 481 6388 E ctn@cdhlegal.com

**NAIROBI**
Merchant Square, 3rd floor, Block D, Riverside Drive, Nairobi, Kenya. P.O. Box 22602-00505, Nairobi, Kenya.
T +254 731 086 649 | +254 204 409 918 | +254 710 560 114
E cdhkenya@cdhlegal.com

**ONGWEDIVA**
Shop No. 94, Oshana Mall, Ongwediva, Namibia
T +264 (0) 81 287 8330 E cdhnamibia@cdhlegal.com

**STELLENBOSCH**
14 Louw Street, Stellenbosch Central, Stellenbosch, 7600.
T +27 (0)21 481 6400 E cdhstellenbosch@cdhlegal.com

**WINDHOEK**
2nd Floor, 4@Steps - East Tower, Hilltop Estate, Kleine Kuppe, Windhoek.
PO Box 97115, Maerua Mall, Windhoek, Namibia, 10020
T +264 833 730 100 E cdhnamibia@cdhlegal.com