Why cybersecurity is needed in farming

By Jyothi Laldas |4 April 2024 | 8:26 am

The farming industry is vital to the world's food industry and requires the utmost protection from cyberattacks. This is according to Carey van Vlaanderen, CEO of ESET Southern Africa, who believes that with the evolution of technology, the digital threat level for farmers has increased in recent years.

"Technology has improved productivity, efficiency and communication in every industry across the globe, and agriculture is no exception. Once considered a traditionally low-tech industry, the increased use of email, online monitoring tools, remote controls and payment systems, together with automated smart farming equipment such as Internet-connected tractors, means the digital threat level has increased for farmers," Van Vlaanderen said.

READ ***Give your farm security a high-tech boost***

"As is the case in many industries across the globe, a growing reliance on online, connected technologies means businesses are more vulnerable to cyberattacks. The

use of smart devices, including sensors and analytics, IoT devices, robotics, drones, and precision farming, have all transformed the agricultural landscape for the better. These tools also gather extensive quantities of sensitive information that could be lucrative to criminals seeking financial gain."

According to a report released in 2023, South Africa ranked number five globally on a list of countries worst affected by cybercrime.

Disruptions in Transnet's IT applications following a cyberattack brought agricultural imports and exports to a standstill in July last year, she explained.

"In a world increasingly reliant on digital technology, the agricultural sector's vulnerability to cyberattacks not only threatens individual agricultural businesses but poses a risk to national food security, making robust cybersecurity measures of critical importance."

Van Vlaanderen emphasised that the threat was not exclusive to South Africa. A University of Cambridge report highlights that smart farming technologies, including automated crop sprayers and robotic harvesters, are susceptible to hacking, and the likelihood of such incidents is on the rise.

She noted that cybercriminals perceived the worldwide dependence on food and agriculture as a vulnerability, seizing the opportunity to launch cyberattacks on the industry for financial gain through ransomware or to cause social and economic disruption.

"Ransomware attacks can be particularly malicious, for example, by erasing backups or threatening to publish confidential information online as a strategy to pressure an organisation into paying the ransom with little risk of being caught and apprehended.

"Today, almost every farmer and agricultural enterprise will use some form of technology to do business. For smaller businesses, simple security solutions such as the automatic updating of software, antivirus software and multi-factor authentication are critical. However, larger, more intensive farming operations using automated farming systems may require more complex security measures."

READ ***How technology is making monitoring animal health easier***

Agriculture in general has historically been shown to have a low level of cyber security in place since attacks are not perceived as being as prevalent as in the financial sector, Van Vlaanderen emphasised.

“There is a prevailing myth among some sectors of the South African farming community that their businesses simply aren’t an attractive target for cybercriminals. But given the vast amounts of data inherent in many agricultural activities, as well as the substantial financial transactions involved, it is preferable to take a proactive approach to digital security in the face of sophisticated cyber threats,” she said.

Although tackling cybersecurity challenges in agriculture may be intricate, she mentioned that agricultural firms could adopt measures to minimise their vulnerability, mitigate the impact of a potential attack, and empower their employees as the primary line of defence.

Identify weak points

“A necessary first step in strengthening defences is to identify where critical infrastructure is vulnerable to attack. This will be different for each business. Some operations may require more investment in cloud security or vulnerability discovery while businesses may need to extend their cybersecurity efforts to include safeguarding themselves from cyberthreats in the form of phishing emails from the companies they partner with and procure from.”

With almost 88% of data breaches being caused by an employee mistake, Van Vlaanderen said a strong human risk management programme with regular employee training and cybersecurity awareness was a crucial element of any cybersecurity strategy.

“Employees can be just as susceptible to cyber threats and should be reminded on an ongoing basis of the risks that are out there and the impact that it can have on them and the farming business.”

She said mistakes, ranging from failure to properly delete data from devices to preventable errors like clicking on links in phishing emails, were preventable.

“From basics such as implementing password managers and using multi-factor authentication to using cutting-edge security technology to withstand an attack on

big farming service companies, much more can be done to ensure farmers are supported with the very best cybersecurity strategies and solutions.”