# Cybersecurity Vulnerabilities in Precision Agriculture

**Ali Mirzakhani Nafchi,** Assistant Professor & SDSU Extension Precision Agriculture Specialist
**Alexander Smart,** Professor & SDSU Extension Agriculture and Natural Resources Senior Program Leader
**Xufei Yang,** Assistant Professor & SDSU Extension Environmental Quality Engineer
**Sushant Mehan,** Assistant Professor & SDSU Extension Water Resource Engineer Specialist
**Jameson Brennan,** Assistant Professor & SDSU Extension Livestock Grazing Specialist

**July 2024**

As Precision Agriculture (PA) evolves, cyber threats become more sophisticated. Adopting a proactive approach to cybersecurity, guided by best practices and standards, is essential for protecting sensitive data and ensuring the resilience of agricultural operations. Continually assessing and updating security practices in response to emerging threats through collaboration, education, and the strategic application of technology, the PA sector can enhance cybersecurity, safeguarding future farming and the food supply chain. PA relies on various digital technologies, including Internet of Things (IoT) devices, Global Positioning System (GPS), and cloud computing, making it susceptible to various cyber threats, as follows:

## Data Breaches

Unauthorized access to agricultural data can reveal sensitive information about farming practices, land use, and crop yields. Embracing PA tools has transformed how farmers grow crops, manage land, and optimize agricultural processes. This digital shift makes farming more efficient but also brings new challenges, especially the risk of data breaches. Sneaking a peek at our farm's secrets could give others an unfair advantage or even threaten the farm's safety and the broader food supply. When sensitive information like crop yields, land use, or financial records gets into the wrong hands, it can be used against us in many ways. Someone might copy our farming strategies, mess with market prices, or even lock our data and ask for ransom. That sounds scary, but the good news is we can fight back with intelligent cybersecurity practices. Think of cybersecurity like the fences and locks on your farm - but for your digital data. By putting up strong defenses, like keeping our software up to date, using complicated passwords, and teaching everyone on the farm about the importance of being careful online, we can keep our digital farm gates locked tight. Just like farming, as we learn about the best technologies or practices, we need to grow our knowledge and defenses in cybersecurity to keep our data, farms, and food supply safe and secure.

## Ransomware Attacks

Malicious software can block access to key data and systems until a ransom is paid, severely disrupting operations. Cyber ransomware threats to our digital farming can put a wrench in our operations, using harmful software to lock away the information we rely on, from soil moisture data to crop yield forecasts,

asking for money to give it back. Here are a few tips to protect our farms and keep our operations smooth: First, staying informed and vigilant is our shield. Knowing how these attacks happen, like through suspicious emails or unsecured Internet connections, can help us steer clear of trouble. It is like learning the signs of a pest infestation but for our computers and devices. Next, keeping our digital tools updated and secure is like locking the barn door at night. We can keep these cyber pests out by updating our software, using antivirus programs, and ensuring our data is as secure as our livestock. Moreover, having a backup of our most important information is like having insurance for our data. It means we can get back on our feet quickly, with minimal fuss and lost time. While the risk of ransomware is real, these approaches are about more than just protecting our farms, also about working together to strengthen our community against these threats.

## Spoofing and Tampering

GPS spoofing, i.e., maliciously distorting location information, can misdirect agricultural equipment, and tampering with data can lead to incorrect agricultural decisions. PA represents the convergence of technology and farming, utilizing GPS, (IoT) devices, and data analytics to revolutionize farm management and efficiency. However, this approach introduces vulnerabilities to cyber threats, especially GPS spoofing and data tampering. GPS spoofing can misguide agricultural machinery, compromising the precision and efficiency of planting, protection, and harvesting operations. Data tampering can corrupt the decision-making process, potentially leading to suboptimal resource utilization and adverse environmental impacts. Even minor deviations can result in significant yield losses and increased operational costs. For instance, automated tractors and drones, which rely on GPS for tasks like seeding or monitoring crop health, can be redirected, causing them to miss target areas or apply inputs twice, wasting resources and potentially damaging crops. Attackers might manipulate data concerning soil moisture levels, crop health, or weather forecasts, leading to misguided decisions, such as overuse or underuse of water, fertilizers, or pesticides, e.g., In 2023, a lot of farmers in Australia and New Zealand were put to halt due to some signal failure that guided their GPS Machinery. The agricultural sector's response requires a comprehensive cybersecurity framework that includes encrypted GPS communications, secure data transmission, and the application of blockchain technology to ensure data integrity. Education is crucial for all stakeholders involved to enhance the sector's resilience to these cyber threats.

## Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

Overloading networks with traffic can render PA systems inoperable, leading to critical delays and financial loss. PA relies heavily on interconnected systems to optimize farm operations through real-time data collection, monitoring, and automated control systems, increasing efficiency, productivity, and sustainability. However, these systems' interconnectedness and online nature expose them to cyber threats, including Denial of Service (DoS) attacks. DoS attacks, particularly damaging within the PA context, can overload networks with traffic, rendering critical systems inoperable and leading to significant operational disruptions and financial losses. A DoS attack aims to flood a network or system with overwhelming traffic, queries, or data packets, making the service unavailable to its intended users. In the context of PA, this could mean the disruption of real-time monitoring and control systems for irrigation, fertilization, and pest control, among others. Such attacks not only halt farm operations but also can lead to crop loss, resource wastage, and a temporary shutdown of agricultural production. Several factors make PA systems vulnerable to DoS attacks. Agricultural systems with limited security features and computational power can be easy targets for attackers. Additionally, the widespread use of standardized communication protocols without adequate security measures can expose the entire network to vulnerabilities if just one device is compromised. Combatting DoS attacks in PA requires a multi-layered approach. Implementing robust security protocols and encryption can protect data integrity and prevent unauthorized access. Networks should be designed with redundancy and the capacity to handle unexpected loads, ensuring that a surge in traffic does not incapacitate the system. Educating farmers and agricultural professionals about the risks and signs of DoS attacks is critical. Awareness can lead to quicker detection and response, mitigating the potential impact. Deploying network monitoring and intrusion detection systems can help identify unusual traffic patterns or spikes in activity, allowing immediate action to counteract potential DoS attacks. Collaboration among technology providers, cybersecurity experts, and implementing effective strategies to safeguard PA systems against DoS and other cyber threats. Prediction of DDoS attacks is possible now.

## Insider Threats

Employees or contractors with access to systems can intentionally or unintentionally cause harm. PA uses digital technologies to monitor and optimize agricultural production processes and introduces vulnerabilities, notably insider threats. Intentional or unintentional insider threats in PA involve anyone accessing the farm's digital systems and data, which might cause harm intentionally or unintentionally. Insider threats pose a significant risk to PA, with the potential to disrupt operations, cause financial loss, and undermine trust in agricultural technologies. Insider threats can manifest in various ways, ranging from the malicious intent of disgruntled employees seeking to sabotage operations to the inadvertent actions of well-meaning staff lacking cybersecurity awareness. Such threats are insidious because insiders already have legitimate access to systems, bypassing many defenses designed to thwart external attacks. In PA, this could mean unauthorized access to sensitive data, alteration of crop management systems, or interference with automated machinery control systems, leading to disrupted operations, financial loss, or even compromised crop integrity. The implications of insider threats in PA are far-reaching. Malicious actions could alter critical data, such as soil or climate conditions, leading to inappropriate farming decisions. For example, changing the parameters for irrigation systems could flood or drought-stress crops. On the unintentional end, an employee might fall prey to a phishing attack, giving attackers access to the network to deploy malware or ransomware, which could halt production and access to vital data. To address these threats, organizations need to foster a security awareness culture; regular training sessions can educate staff and contractors on the importance of cybersecurity and its role in safeguarding the organization's digital assets. Implementing strict access controls and privilege management ensures that individuals have only the access necessary for their roles. This principle of least privilege can significantly mitigate the potential damage insiders can cause. Monitoring and logging access to sensitive systems can also help detect unusual activities that may indicate insider threats. AI, computer training, and machine learning tools can help identify potential insider threats by detecting anomalies in patterns. This approach can alert organizations to issues before they escalate into serious security incidents. By prioritizing cybersecurity and establishing clear policies and procedures, leaders can create an environment where security is a shared responsibility. Continuous evaluation and adaptation of security strategies are necessary to respond to evolving threats and the changing landscape of PA.

## Summary

PA integrates advanced digital technologies, such as IoT devices, GPS, and cloud computing, making it increasingly susceptible to a broad spectrum of cyber threats. These include data breaches, which expose sensitive information; ransomware attacks that encrypt data for ransom; spoofing, which involves masquerading as a trusted entity; tampering with data integrity; denial of service attacks that disrupt service availability; and insider threats from within the organization. To counter these vulnerabilities, we need to embrace a holistic cybersecurity strategy. This strategy should include regular software updates to patch vulnerabilities, the implementation of robust, complex passwords to prevent unauthorized access, encryption to protect data confidentiality, continuous network monitoring to detect and respond to threats in real time, and extensive staff education on cybersecurity best practices. Such comprehensive measures are necessary for protecting sensitive data, ensuring the continuity of farm operations, enhancing the system's resilience against cyber threats, and securing the future of PA and the food supply chain.

South Dakota State University Extension

SOUTH DAKOTA STATE UNIVERSITY®
AGRONOMY, HORTICULTURE & PLANT SCIENCE DEPARTMENT



Learn more at extension.sdstate.edu.



P-00303