USAID
FROM THE AMERICAN PEOPLE

Cybersecurity

AGRICULTURE AND FOOD SECURITY

Photo credit: Ataur Rahman for DAI.

Why Does Cybersecurity Matter for Agriculture and Food Security?

Digital technologies have the potential to boost agricultural productivity to meet global food demand. Internet-enabled sensors allow farmers to gather vast amounts of real-time data on growing conditions, drought, and pest control that can inform future decisions. Many farmers in the countries where USAID works also rely on digital services to gain access to loans, sell their harvest, and set aside money that can help them resist shocks. However, with the obvious benefits of digital agriculture come new risks. Insecure or poorly designed digital agricultural devices or applications can be hacked, potentially exposing sensitive data—including Personal Identifiable Information (PII)—to cyber criminals or other malign actors. These data breaches can pose significant risks for farmers and other members of the agricultural value chain, including identity theft and loss of assets. USAID and other donors that are increasingly using digital solutions in agricultural programming must identify and mitigate potential threats to program participants. On a macro scale, cyber attacks can threaten global food security. Attacks on smart farming and on precision agriculture devices can threaten yields and, if mounted on a large enough scale, can pose a serious risk of widespread hunger and economic damage at a local, regional, or even national level. While most farmers USAID works with are not at this level of agricultural automation, this is a challenge that USAID and its partners should consider for the future.

Growing digitization of the agriculture and food security sector increases the number of cyber threats and risks, such as ransomware. The growth of precision agriculture and smart farming has rapidly increased the number of Internet-enabled devices in the agriculture sector, which increases the cyber attack surface or the number of potential entry points for a cyber attacker. Ransomware is a particular concern. Easily deployable ransomware attacks, in which cybercriminals threaten to destroy farmers' data and systems unless a ransom is paid, will become more common on critical data and equipment, particularly during time-sensitive windows for planting and harvesting. The weaker, more exploitable links in the chain of Internet of Things (IoT) devices will be used as a stepping stone to gain access to connected systems further up the supply chain, leading to much broader risks such as sector-wide cyber attacks on agriculture.

What is cybersecurity, and why does it matter for international development?

As noted in USAID's Cybersecurity Primer, USAID defines cybersecurity as "the activity or process, ability or capability, or state whereby information and communications systems that support or affect development outcomes, and the information contained therein, are protected from and/or defended against damage, unauthorized use or modification, or exploitation." As USAID partner countries further their digital transformation and continue to adopt new digital tools and systems, cyber risks and vulnerabilities proliferate. Cybersecurity failures pose material threats to USAID partner countries and undermine partner country government legitimacy. USAID must protect its digital investments by ensuring that its digital programming addresses cyber harms and includes cybersecurity mitigation measures.

Russian hackers lay the groundwork to attack an agricultural producer in Ukraine

In April 2022, Microsoft reported that Sandworm (a cyber threat actor attributed to a Russian military intelligence unit) reportedly placed a file encryptor on the network of a Ukrainian agricultural producer during the early stages of the war. Though not yet activated, this file encryptor means that this agricultural company—which Microsoft speculates to be a grain producer, given the importance of this crop to Ukraine's economy—is at higher risk of attack in the future. Ukraine is also using agricultural technology to its advantage. After a John Deere outlet was looted by Russian troops in Melitopol, an unidentified group of Ukrainians enabled a "kill switch" that made the machinery unusable.

What is the Internet of Things?

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) defines IoT as "any object or device that sends and receives data automatically through the Internet." Common IoT devices include smart doorbells like Nest, fitness trackers like Fitbit, and smart home security systems. IoT devices in the agriculture and food security sector include weather stations, smart farming sensors (such as for irrigation), greenhouse automation systems, crop management devices, and smart collar tags for livestock.

The move to smart farming and precision agriculture generates significant data, which is also open to cyber risks. The growing use of automated machinery, high resolution multispectral imagery, drones, soil sensors, and IoT technologies in the agriculture and food security sector is generating large amounts of data. This renders the sector highly vulnerable to data theft and manipulation, creating a wide range of possible threat vectors. Cybercriminals could steal, manipulate, and then publish false and harmful agricultural data to undermine local industry. Foreign governments can use another country's agricultural data to give themselves an advantage in trade negotiations or commodities markets. In some cases, the agricultural applications and databases might not be the ultimate target of the attacker. In 2021, cybersecurity researchers discovered a sprawling cyber attack against six U.S. states. The attackers, thought to be associated with the People's Republic of China, initially gained access to state networks through USAHerds, an app that helps state governments track livestock diseases. When digital agriculture applications are insecure, they can serve as open doors to other networks, allowing hackers to gain access to sensitive information such as health, finance, and government data.

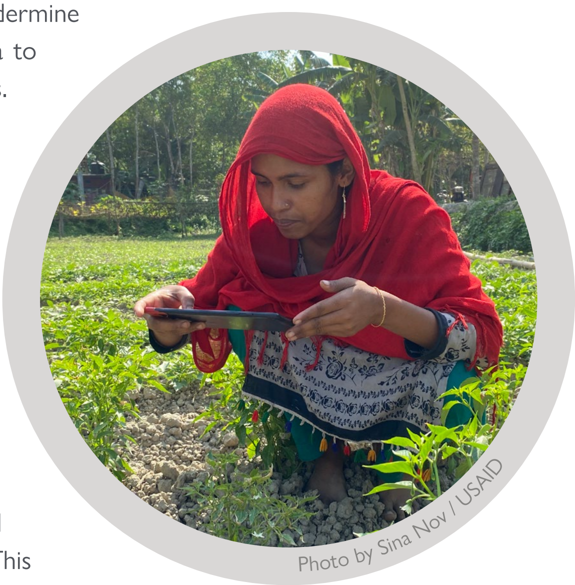
Photo by Sina Nov / USAID

Many national level cybersecurity and data privacy laws in low- and middle-income countries (LMICs) do not cover agricultural technology. The policy space governing agricultural technologies—particularly data generated by these devices—is largely unregulated in many USAID partner countries. This further increases cyber-related risks. For example, although data privacy and data use policies and regulations (which govern the agriculture sector) are in place at the regional level in Africa through the African Union and its regional economic communities, they often do not extend to the national level on the continent. This is not true in all countries. Ghana's 2014 national cybersecurity policy underscores the importance of agriculture to the country's economy and well-being, recognizing the potentially disastrous consequences of an attack on the sector. Similarly, the Innovation and Cybersecurity Department of the Rwanda Utilities Regulatory Authority is mandated to help various sectors of Rwanda's economy—including the agriculture sector—incorporate new technologies into their work, including e-agriculture, IoT, and big data.

What does the Bureau for Resilience and Food Security Digital Strategy Action Plan say about cybersecurity?

> "RFS intends to…ensure that cyber hygiene practices have been defined for programmatic activities and require implementing partners to identify measures they are taking to mitigate threats associated with digital tools as well as help identify cybersecurity threats in the countries in which they work."

Key Considerations for Cybersecurity Activities in Agriculture and Food Security

- Understand partner country policies, strategies, and regulations around cybersecurity, data privacy, communications infrastructure, and digitalization.
  - USAID Missions and Bureaus must understand the cybersecurity ecosystems they are operating in before designing and implementing new activities. Digital Ecosystem Country Assessments (DECAs) are one mechanism for better understanding these dynamics. If your Mission does not have a DECA, consider commissioning one.
  - For a more specific understanding of digital agriculture, consider requesting a digital agriculture ecosystem assessment from RFS. Please reach out to digitalag@usaid.gov to learn more.
- Embed cybersecurity considerations, resources, responsibilities, and management tools into every project or activity in the agriculture and food security sector.
- Continue to prioritize digital literacy and cyber hygiene training that help agricultural program partners understand topics like navigating privacy settings, identifying and avoiding phishing attempts, and using technology safely and responsibly. If specific partners need cyber hygiene training, consider buying into USAID's Digital APEX mechanism, which provides cybersecurity support to USAID partners. Use the email address below to contact the team for details.
- Protect agriculture and food security-specific digital tools and solutions. Missions and Bureaus might consider buying into USAID's Digital APEX mechanism to conduct a full vulnerability assessment of any new or existing agricultural tools. Digital APEX experts recently conducted a vulnerability assessment—including penetration testing–of tools developed by RFS implementing partners. Think of penetration testing as ethical hacking It simulates a real attack on a computer system to identify any gaps and weaknesses in security. An understanding of these weaknesses can help the system administrator patch vulnerabilities and improve the overall security of the system. If you are interested in learning more about Digital APEX services, use the email address below.

Photo by Riaz Jahanpour for USAID / Digital Development Communications

TO LEARN MORE about cybersecurity and USAID programming, please reach out to USAID's Cybersecurity Team at cybersecurity.itr@usaid.gov and the RFS digital team digitalag@usaid.gov.