September 28, 2023

MIAC

Missouri Information Analysis Center

Cybersecurity Intelligence Bulletin

(U//PAB) Internet of Things (IoT) in Agriculture - A Beginner's Guide

(U//PAB) Scope

(U//PAB) The introduction of smart devices, also known as Internet of Things or (IoT) devices, to the Agricultural sector, has increased efficiency, productivity, and sustainability. An IoT device is "a network of physical devices, vehicles, appliances and other physical objects that are embedded with sensors, software and network connectivity that allows them to collect and share data."[i] In the Agriculture sector, IoT would be any device connected to the internet that collects, monitors, and analyzes data. While IoT brings large benefits to the sector, it also widens the risk landscape. This product will give examples of IoT on the farm, IoT considerations, highlight some of the cybersecurity risks IoT adds to the sector, IoT & Ag in the news, and provide resources.

(U//PAB) IoT on the Farm

(U//PAB) Today, there are many IoT applications and/or devices used in agriculture.
Examples include:

- Climate based solutions such as sprayers
- Weather stations (allMETEO, Smart Elements, Pycno)
- Greenhouse automation (Farmapp, Growlink)
- Facility management solutions such as Farm Productivity Management Systems (FarmLogs, Cropio)
- Crop management (Arable, Semios)
- Cattle monitoring (SCR by Allflex, Cowlar)
- Data driven solutions such as Precision Farming (CropX, Mothive)
- Predictive analytics for smart farming (Crop Performance, SoilScout)
- Drones (Sense Fly, DroneSeed for deforestation recovery)
- Automation (Bear Flag Robotics, Eco Robotics)[1]

(U//PAB) IoT Considerations

(U//PAB) With IoT entering the Agriculture sector, professionals in this industry should consider who owns the data that is being gathered by the IoT device. When the supplier installs a monitoring device on a grain silo to measure the volume and schedule deliveries, the data set is as much about the farm, as it is about the grain logistics. Therefore, who owns the data, where is it stored, and what is it used for are questions which should be consided prior to utilzing an IoT device.

(U//PAB) As of December 31, 2021 the Farm Service Agency reports 433,213 acres of Missouri agricultural land is being held by foreign investors (54% of which is cropland, 23% is pasture). This number increased from 393,546 in 2020.[ii] Since IoT in the Agriculture sector is still new, policies that govern data ownership have yet to be created, yet when investing in equipment these are questions the suppliers should be able and willing to answer concerning their IoT products.

(U//PAB) Secondly, consider vetting vendors to ensure you are buying IoT devices that are effective and can be secured.

(U//PAB) Some best practices include: [iii]

- Have an in-person or video call
- Review vendor performance on other platforms

If any member of the public has pertinent information regarding the subject material contained within this Public Awareness Bulletin, they should contact the agency listed above directly. This information may be copied and distributed to the public. Any unauthorized alteration of any portion of this Public Awareness Bulletin is considered a violation and subject to legal prosecution.

- Establish Know Your Business (KYB)
- Compliance checks (Such as SOC II or HITRUST)
- Full comprehesive due dilligence (risk assessment)
- Certification validation

(U//PAB) Lastly, some characteristics to consider in IoT devices include the large number of devices which may be needed, their lifespan, and the total cost of ownership. The entire life cycle of the product must be considered; procurement, installation, maintenance, and removal. If thousands are being deployed, the cost can amount to a significant sum of money.

(U//PAB) When identifying the total cost of ownership of IoT devices, it is important to take into account:[iv]

- Installation costs
- Device maintenance (changing out batteries, fixing faults, performing upgrades)
- Maintenance cost
- Cost of transmitting the data
- Cost of storing and analyzing the data
- Any costs associated with decommissioning devices

(U//PAB) IoT Cybersecurity Risks

(U//PAB) Ransomware is a concern for any device that is connected to the internet. "Ransomware is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyber attackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files. Some variants have added additional functionality – such as data theft – to provide further incentive for ransomware victims to pay the ransom."[v]

(U//PAB) "Ransomware has quickly become the most prominent and visible type of malware. Recent ransomware attacks have impacted hospitals' ability to provide crucial services, crippled public services in cities, and caused significant damage to various organizations."[vi]

(U//PAB) Ransomware can lead to data breaches; this is when personal sensitive information is posted to or sold on the internet or dark web. Some of the sensitive data that can be released or sold in a breach are usernames and passwords to multiple websites, such as social media, banks, email, business accounts, utilities, etc. If passwords are duplicated for IoT devices, applications, and/or websites and are leaked, bad actors can use those credentials to access additional data. This is called credential stuffing, "the automated injection of stolen username and password pairs ("credentials") into website login forms, in order to fraudulently gain access to user accounts."[vii]

(U//PAB) The Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) has produced a document on how to prevent ransomware attacks and how to protect sensitive data (https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf). However, sometimes you are not in control of the data, for example with IoT devices. Going back to the above section on IoT Considerations, such as where is your data being stored and who has ownership. The cybersecurity risks identified by CISA, to include many more, are the reasons it is important to know the answers to these questions. Once data has been breached, there is no way to get it back, the best thing to do is to try to prevent a data breach before it happens. We all know data breaches will happen; the goal is to minimize the impact when they do.

(U//PAB) IoT & Ag in the News

- Internet of Cows: Ingestible IoT Sensor Monitors the Health of Livestock https://www.iottechnews.com/news/2021/nov/02/internet-of-cows-ingestible-iot-sensor-monitors-health-livestock/
- Cyber Threats Impacting the Food and Agriculture Sector https://www.food-safety.com/articles/8800-cyber-threats-impacting-the-food-and-agriculture-sector

- Cybersecurity Report: “Smart Farms” Are Hackable Farms https://spectrum.ieee.org/cybersecurity-report-how-smart-farming-can-be-hacked
- Cyber Threats Facing Agriculture: Bad Actors Looking to Dine Out on Farm Data https://techhq.com/2022/08/security-warning-cyber-attacks-against-agriculture/
- How are Farmers Using Blockchain, AI and IoT? AMA with Dimitra https://cointelegraph.com/news/how-are-farmers-using-blockchain-ai-and-iot-ama-with-dimitra
- University of Missouri Gets Midwest’s First Autonomous Tractor https://www.missourinet.com/2023/09/20/university-of-missouri-gets-midwests-first-autonomous-tractor/

(U//PAB) IoT Resources

(U//PAB) In conclusion, it is important to know the risk landscape when introducing IoT to your farm. You need to know what to protect from, to protect yourself, your farm, your data, and your livelihood adequately. Below is a list of recommendations, best practices, frameworks, and product labels to further explain IoT in the Agriculture sector. The list begins with resources meant to be applicable to farmers considering purchasing IoT devices, while the list concludes with resources designed for larger scale operations to establish policy and standardized frameworks.

(U//PAB) Pre-Purchase Resources

- US Department of Homeland Security
  - CISA Internet of Things (IoT) Acquisition Guidance Document: https://www.cisa.gov/resources-tools/resources/internet-things-iot-acquisition-guidance-document
- Federal Trade Commission: https://www.ftc.gov/business-guidance/resources/careful-connections-keeping-internet-things-secure
- Carnegie Melon University IoT Security and Privacy Label Program: IoT Security and Privacy Label

(U//PAB) Post-Purchase Resources

- FBI IoT Public Service Announcement: https://www.ic3.gov/Media/Y2018/PSA180802
- Microsoft Defender for IoT: https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/concept-enterprise
- Digi IoT Devices Security in Five Simple Steps: https://www.digi.com/resources/videos/iot-device-security-in-five-simple-steps

(U//PAB) Frameworks and Governance

- National Institute of Standards and Technology (NIST):
  - US NIST: Draft Security Feature Recommendations for IoT Devices – https://www.nist.gov/news-events/news/2019/08/nist-releases-draft-security-feature-recommendations-iot-devices
  - US NIST: Draft Security Feature Recommendations for IoT Devices – https://www.nist.gov/news-events/news/2019/08/nist-releases-draft-security-feature-recommendations-iot-devices
  - US NIST: 8259A IoT Device Cybersecurity Capability Core Baseline
  - US NIST: 8259B IoT Non-Technical Supporting Capability Core Baseline
  - US NIST: Systems Security Engineering 800.160: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
  - US NIST: IoT https://www.nist.gov/topics/internet-things-iot
  - US NIST: Recommended Criteria for Cybersecurity Labeling for Consumer IoT Products
- Cloud Security Alliance (CSA): Future-proofing the connected world: 13 steps to Developing Secure IoT Products: https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf
- IoT Security Foundation:
  - IoT Security Foundation: Whitepaper: Establishing Principles for IoT Security: https://iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf

  - IoT Security Foundation: IoT Security Assurance Framework: https://iotsecurityfoundation.org/best-practice-guidelines/
- US Department of Homeland Security
  - US Department of Homeland Security: Strategic Principles for Securing the Internet of Things: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf

(U) Sources

[i](U) https://www.ibm.com/topics/internet-of-things
[ii] (U)https://www.fsa.usda.gov/Assets/USDA-FSA-Public/usdafiles/EPAS/PDF/2021_afida_annual_report_through_12_31_2021.pdf
[iii] (U)https://www.nauticalcommerce.com/blog/vet-marketplace-vendors
[iv] (U)https://www.betasolutions.co.nz/blog/20-things-to-consider-when-planning-an-iot-solution-part-1
[v] (U)https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/#:~:text=Ransomware%20is%20a%20malware%20designed,regain%20access%20to%20their%20files.
[vi] Ibid.
[vii] (U)https://owasp.org/www-community/attacks/Credential_stuffing

If any member of the public has pertinent information regarding the subject material contained within this Public Awareness Bulletin, they should contact the agency listed above directly. This information may be copied and distributed to the public. Any unauthorized alteration of any portion of this Public Awareness Bulletin is considered a violation and subject to legal prosecution.