“Cyber Threats to Precision Agriculture”

Moderator
Daniel Eliot,
Director Small Business Education
National Cyber Security Alliance

Speaker
Mike Matson,
Intelligence Analyst
Federal Bureau of Investigation

Speaker
Pete Mutschler
Director, Environment, Health and Safety, CHS Inc.
& Secretary of the Board of Directors for ResponsibleAg.
Goal of 5-Step Approach Is Resilience

- Know the threats and Identify your assets
- Detect problems and respond quickly and appropriately
- Know what recovery looks like and prepare

Thanks to our National Sponsors

TREND MICRO

Initiative for Education

INFOSEC
Threats to Precision Agriculture

Presenters:
Pete Mutschler, CHS Inc. & ResponsibleAg
Mike Matson, FBI Louisville Field Office
Webinar Outline

- Precision Agriculture Defined for This Webinar
- Analyst Exchange Program’s ‘Threats to Precision Agriculture’ Project Reviewed
- Key Findings of the Final Report Published by DHS
- Best Practices in Cyber Security Applicable to Precision Agriculture
What is Precision Agriculture?

- **Precision Agriculture 1.0**
  - Farming became tech dependent 1960s
  - PA began late 1980s
  - Exploited GPS Technologies
  - Yield Monitoring / Maps
  - Variable Rate Technologies
  - Variable Rate Applications

- **Precision Agriculture 2.0 “Smart Farming”**
  - Advanced Exploitation of PNT Systems
  - Internet Connected
  - Multiple Communication Technologies
  - Sensor Intensive / Sensors Everywhere
  - Data Intensive
  - Data Analytics
  - Advanced Techniques: Machine Learning, Mesh Networks, Edge Computing
Analyst Exchange Program Explained

- Annual Office of Director of National Intelligence program run by DHS to bring together experts from the private sector and government to research forward looking topics.
- 2018 AEP program had multiple topics, one of which was “Threats to Precision Agriculture.”
- Research lasted six months, including field research trip to Midwest.
- Participants in the group included experts from:
  - Private Sector: CHS Inc, ResponsibleAg, and Thompson Reuters.
  - State Government: Northern California Regional Intelligence Center.
Key Findings

- The project uncovered potential threats using the **Confidentiality**, **Integrity**, and **Availability** information security model. These threats have a potential to:
  - Potential to weaken agriculture’s resiliency to chronic stresses and acute shocks.
  - Significantly increases the scale and scope of legacy threats.

- Precision agriculture technology is introducing new vulnerabilities into the industry.

- Precision agriculture dramatically increases the agriculture sector’s attack space.

- Different vulnerabilities within CIA model identified across agriculture subsectors.
<table>
<thead>
<tr>
<th>Sector</th>
<th>Impact: Data Confidentiality</th>
<th>Impact: Data Integrity</th>
<th>Impact: Equipment Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Row Crops</td>
<td>Yield Data / Cost Data</td>
<td>Soil Data / Yield Data</td>
<td>Major Farm Equipment</td>
</tr>
<tr>
<td>Vegetables</td>
<td>Yield Data / Cost Data</td>
<td>Soil Data / Yield Data</td>
<td>Major Farm Equipment</td>
</tr>
<tr>
<td>Fruits</td>
<td>Yield Data / Cost Data</td>
<td>Automatic Water Systems DSS Equipment</td>
<td>Robotic Picking Equipment Water Pivots</td>
</tr>
<tr>
<td>Nuts</td>
<td>Yield Data / Cost Data</td>
<td>Automatic Water Systems DSS Equipment</td>
<td>Robotic Picking Equipment Water Pivots</td>
</tr>
<tr>
<td>Unique Value (Vineyards / Ginseng / Hemp)</td>
<td>Plant Genetics</td>
<td>Automatic Water Systems</td>
<td>Cellar Climate Systems Water Pivots</td>
</tr>
<tr>
<td>Beef Cattle</td>
<td>Breeding Data</td>
<td>Animal Health Data</td>
<td>DSS Equipment</td>
</tr>
<tr>
<td>Dairy Cattle</td>
<td>Breeding Data / Yield Data</td>
<td>Animal Health Data</td>
<td>Robotic Milking Equipment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Robotic Milking Barns</td>
</tr>
<tr>
<td>Swine</td>
<td>Breeding Data / Yield Data</td>
<td>Animal Health Data</td>
<td>Smart Barns</td>
</tr>
<tr>
<td>Poultry</td>
<td>Breeding Data / Yield Data</td>
<td>Animal Health Data</td>
<td>Barn Climate Systems</td>
</tr>
<tr>
<td>Unique Value (Horses)</td>
<td>Breeding Data</td>
<td>Animal Inputs</td>
<td>Barn Climate Systems</td>
</tr>
</tbody>
</table>
Threats to Confidentiality

- Intentional theft of data collected through decision support systems such as tablets and apps, or the unintentional leakage of data to third parties.
- Intentional publishing of confidential information from within the industry such as from a supplier to damage the company or cause chaos.
- Foreign access to unmanned aerial system data.
- Unscrupulous sale of confidential data.
Threats to Integrity

- Intentional falsification of data to disrupt crop or livestock sectors.
- Introduction of rogue data into sensor networks damaging a crop or herd.
- Insufficiently vetted machine learning modeling.
Threats to Availability

- Timing of equipment availability.
- Disruption to positioning, navigation and timing systems – space based.
- Disruption to positioning, navigation and timing systems – ground based.
- Disruption to communication networks.
- Foreign supply chain access to equipment used in precision agriculture.
- Smart livestock production facility failure.
Impact - Government

- Mass disabling of connected equipment could have an impact on food security if the timing of the attack hit during planting or harvesting.

- A foreign government could identify and obtain close up imagery of critical infrastructure through foreign access to equipment sensor data.

- A deep fake scenario which triggered a regulatory response could have interstate commerce and foreign trade implications.
Impact – Private Sector

- Highest impacts all revolve around loss to the individual farmer: equipment, yield, time; money.
- Reputational loss to equipment & software manufacturers.
- Loss of consumer confidence in food and agriculture industry.
Best Practices

- While threats to precision agriculture technologies are specific to industry, baseline security controls necessary to mitigate threats are consistent with other industries.

- Recommended best practices are derived from the Center for Internet Security’s critical security controls (http://www.cisecurity.org/controls/) and additional guidance from industry practitioners. Examples:
  - Implement Email and Web Browser Protections
  - Limit and Control Network Ports, Protocols, and Services
  - Inventory and Control Hardware and Software Assets
  - Account Monitoring and Control
  - Separate Operational Technologies and Business Operations
  - Data Recovery Capabilities
  - Incident Response and Management
  - Implement Physical Controls
### Basic
1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

### Foundational
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

### Organizational
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

---

This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License (the link can be found at https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode).

To further clarify the Creative Commons license related to the CIS Controls™ content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform or build upon the CIS Controls, you may not distribute the modified materials. Users of the CIS Controls framework are also required to refer to (http://www.cisecurity.org/controls/) when referring to the CIS Controls in order to ensure that users are employing the most up to date guidance. Commercial use of the CIS Controls is subject to the prior approval of CIS® (Center for Internet Security, Inc.).
<table>
<thead>
<tr>
<th>CIS Sub-Control</th>
<th>Asset Type</th>
<th>Security Function</th>
<th>Title</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>Applications</td>
<td>Protect</td>
<td>Ensure Use of Only Fully Supported Browsers and Email Clients</td>
<td>Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.</td>
</tr>
<tr>
<td>7.2</td>
<td>Applications</td>
<td>Protect</td>
<td>Disable Unnecessary or Unauthorized Browser or Email Client Plugins</td>
<td>Uninstall or disable any unauthorized browser or email client plugins or add-on applications.</td>
</tr>
<tr>
<td>7.3</td>
<td>Applications</td>
<td>Protect</td>
<td>Limit Use of Scripting Languages in Web Browsers and Email Clients</td>
<td>Ensure that only authorized scripting languages are able to run in all web browsers and email clients.</td>
</tr>
<tr>
<td>7.4</td>
<td>Network</td>
<td>Protect</td>
<td>Maintain and Enforce Network-Based URL Filters</td>
<td>Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.</td>
</tr>
<tr>
<td>7.5</td>
<td>Network</td>
<td>Protect</td>
<td>Subscribe to URL-Categorization service</td>
<td>Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.</td>
</tr>
</tbody>
</table>
Best practices can be implemented at every level, creating defense in depth and building resiliency into Precision Agriculture networks.
Questions?
Contact Information:

Pete Mutschler
CHS Inc. and ResponsibleAg
Pete.Mutschler@chsinc.com

Mike Matson
FBI Louisville Field Office
mvmatson@fbi.gov
Cyber Threats to Precision Agriculture

Founding Sponsor
FedEx
smallbusiness.fedex.com

Signature Sponsor
Trend Micro
www.trendmicro.com

Contributing Sponsor
Infosec
www.infosecinstitute.com

To access the report from today:
https://www.us-cert.gov/ncas/current-activity/2018/10/03/Cybersecurity-Threats-Precision-Agriculture

National Cyber Security Alliance
www.staysafeonline.org/cybersecure-business