Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

This PIN is a joint product by the Federal Bureau of Investigation and the US Department of Agriculture.

31 March 2016

PIN Number
160331-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

Smart Farming May Increase Cyber Targeting Against US Food and Agriculture Sector

Summary

The FBI and the US Department of Agriculture (USDA) assess the Food and Agriculture (FA) Sector is increasingly vulnerable to cyber attacks as farmers become more reliant on digitized data. While precision agriculture technology (a.k.a. smart farming)[a] reduces farming costs and increases crop yields, farmers need to be aware of and understand the associated cyber risks to their data and ensure that companies entrusted to manage their data, including digital management tool and application developers and cloud service providers, develop adequate cybersecurity and breach response plans.

Threat

The FBI and USDA assess the farming industry's growing adoption of precision agriculture technology may increase cyber targeting activity against the FA Sector with the intent to steal farm-level data in bulk. A recent example of government-authorized big data analytics demonstrates the value of aggregating farm-level data to track and even anticipate crop availability and pricing. Similarly, criminals could aggregate stolen data or steal analyzed data to exploit US agriculture resources and market trends.

- *The Wall Street Journal* in March 2014 reported concerns that the FA Sector will face increased cyber targeting with the growing adoption of equipment and services that collect and analyze farm-level data, including information about soil

[a] Precision agriculture, or smart farming, includes the use of sensor technologies to monitor and measure factors contributing to crop growth, with the goal to farm more efficiently.

content and past crop yields as well as planting recommendations (i.e., precision agriculture).[1]

- On 27 January 2016, the USDA announced the winners of a contest in which Microsoft hosted a century of public climate and crop data for competitors worldwide to design data visualization tools for farmers. For example, the winning tool allows users to follow trends in local crop availability and prices. The intent of the contest was to explore how to render big data in agriculture into a tool that allows farmers to make sustainable decisions that have an impact on food supply.[2]

Other Potential Cyber Risks to Farm-Level Data

In addition to theft, farm-level data may also be vulnerable to ransomware and data destruction. Ransomware has become a significant threat to US businesses and individuals. Perpetrators use ransomware to encrypt a user's important files, rendering them unreadable until a ransom is paid. Hacktivists may also destroy data to protest, for example, the use of genetically-modified organisms (GMOs) or pesticides.

The single most important protection measure against these threats is to implement a robust data back-up and recovery plan. Back-ups should be maintained in a separate and secure location so that malicious actors cannot readily access them from local networks.

Historically, the farming industry has lacked awareness of how their data should be protected from cyber exploitation, likely reflecting low industry demand for adequate cybersecurity. In fact, drone manufacturers are focused on offering low pricing structures for farmers by developing data platforms that are interoperable with legacy systems, a hallmark of networked devices with poor cybersecurity (see text box).

- A 2014 American Farm Bureau Federation (Farm Bureau) survey of nearly 3,400 farmers found over half the respondents intended to invest in precision agriculture over the next two years. However, almost 76% of respondents were worried unauthorized individuals could use their data for commodity market speculation, and only about 5% were even aware that the companies holding their data had a security breach response plan.[3, 4]

- *CyberTrend* in January 2016 reported that drone manufacturers offering analytics packages are mindful of farmers' demand for interoperable data platforms in order

to keep pricing low. For nearly a decade, farmers have used drone RGB (red, green, blue) photography and thermography to monitor crop growth. Drone data can be integrated with other precision technology data to inform more efficient farming decisions, but farmers may forgo this capability if new drones require system upgrades that are too expensive.[5]

Lessons from the Healthcare and Public Health (HPH) Sector

In October 2014, the US Food and Drug Administration (FDA) sponsored a public workshop to discuss the cybersecurity challenges facing the HPH Sector. With regard to medical device manufacturing, expert panelists discussed how hospitals' financial constraints and focus on patient safety and convenience have resulted in the improper use of legacy devices and a high demand for user-friendly, interoperable devices. This industry pressure has resulted in manufacturers prioritizing usability over security, thereby rendering connected hospital networks vulnerable to cyber attacks. Panelists discussed how industry leaders' procurement demands—or "market pressures"—for manufacturers to prioritize device cybersecurity very likely are the key to ensuring cybersecurity standards are raised for medical devices overall.

Source: Capital Reporting Company; "Public Workshop: Collaborative Approaches for Medical Device and Healthcare Cybersecurity; Tuesday, October 21, 2014"; 15 December 2014; http://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsConferences/UCM426854.pdf; accessed on 9 March 2016; Transcript for the first day of the FDA-sponsored public workshop on medical device and healthcare cybersecurity.

Fortunately, FA Sector leadership has prioritized enhancing cybersecurity awareness within the sector, and some companies are beginning to invest more in cybersecurity.

- *Homeland Security News Wire* in February 2014 reported major seed and farm equipment providers are investing in stronger cybersecurity as the farming industry increasingly relies on digitized data and the frequency and sophistication of cyber attacks increases. For example, Monsanto was working to improve its cyber defenses after its acquired farm analytics firm, The Climate Corporation, was hacked in 2014 for unspecified reasons that the company did not believe to be related to credit card fraud.[6]

- DHS' new FA Sector-Specific Plan (SSP) describes the sector's acknowledgment of the potential consequences of a successful cyber attack, especially against Industrial Control Systems (ICS) in food production and processing facilities. One of the 2015-2019 sector goals is to assess all-hazards, including cybersecurity, risks to the sector.

A priority in furtherance of this goal is to evaluate and raise awareness of potential cyber risks to the sector and to encourage its members to adopt the NIST Cybersecurity Framework. The SSP notes that many sector owners and operators who are not dependent on ICS do not consider cyber threats to be a serious risk. As such, the Cybersecurity Assessment & Risk Management Approach (CARMA), led by the DHS Office of Cybersecurity and Communications with input from FA Sector stakeholders, aims to produce an assessment of the cyber risks to the broader sector and best practices for risk mitigation.[7]

Recommendation

The purpose of this Private Industry Notification is to increase US farmers' awareness of the cyber risks to farm-level data collected through smart farming. Farmers are encouraged to inquire how data management companies use and protect their data and to be mindful of the cybersecurity features implemented in precision agriculture technology. Precautionary measures that companies should use to mitigate computer intrusion threats include the following:

- Monitor employee logins that occur outside of normal business hours.
- Use two-factor authentication for employee logins, especially remote logins.
- Create a centralized Information Technology e-mail account for employees to report suspicious e-mails.
- Provide regular training to remind and inform employees about current social engineering threats.
- Monitor unusual traffic, especially over non-standard ports.
- Monitor outgoing data, and be willing to block unknown IP addresses.
- Close unused ports.
- Utilize a Virtual Private Network (VPN) for remote login capability.

The FBI and USDA recommend that all FA Sector firms refer to the US Computer Emergency Readiness Team Web site (http://www.us-cert.gov) for additional cybersecurity information and resources.

Reporting Notice

The FBI and USDA encourage recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or e-mail at CyWatch@ic.fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at NPO@ic.fbi.gov or 202-324-3691.

Administrative Note

This product is marked TLP: GREEN. The information in this product is useful for the awareness of all participating organizations as well as for peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels. No portion of this product should be released to the media, posted to public-facing Internet Web sites, or transmitted over non-secure, external communications channels.

There is no additional information available on this topic at this time. For comments or questions related to the content or dissemination of this product, please contact CyWatch.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey

Endnotes

[1] Online newspaper article; *The Wall Street Journal*; "Agriculture Giants Boost Cybersecurity to Shield Farm Data"; 4 March 2014; http://www.wsj.com/articles/agriculture-giants-boost-cybersecurity-to-shield-farm-data-1424380098; accessed on 10 September 2015; The article is based on interviews with agricultural industry experts.
[2] Online news article; *FWC.com*; "How USDA crowdsourced agricultural data"; 27 January 2016; https://fcw.com/articles/2016/01/27/usda-microsoft-contest.aspx; accessed on 1 March 2016; The article is based on an interview with Agriculture Secretary Tom Vilsak concerning the USDA-Microsoft Innovation Challenge.
[3] Online news article; *American Farm Bureau Federation*; "American Farm Bureau Survey Shows Big Data Use Increasing, Big Questions Remain"; 21 October 2014; http://www.fb.org/newsroom/news_article/178/; accessed on 3 November 2015; Source is the American Farm Bureau Federation, a US nonprofit farm organization. The article summarizes key findings from a survey of 3,380 farmers conducted from late July to early September 2014.
[4] *Op. cit.,* endnote 1.
[5] Online news article; *CyberTrend*; "Agriculture & The Internet Of Things: Sensors, Drones, Robotics & Analytics Are Transforming Farming Methods"; 13 January 2016; http://www.cybertrend.com/article/19777/agriculture-and-the-internet-of-things; accessed on 1 March 2016; The article includes professional insights from a senior research analyst at Gartner.
[6] Online news article; *Homeland Security News Wire*; "Agro cyber vulnerability: U.S. farming sector increasingly vulnerable to cyberattacks"; 20 February 2015; http://www.homelandsecuritynewswire.com/dr20150220-u-s-farming-sector-increasingly-vulnerable-to-cyberattacks; accessed on 19 August 2015; The article is based on reporting from a farm-outlook forum hosted by the USDA and a Wall Street Journal interview with Monsanto's chief technology officer.
[7] DHS; Sector-Specific Plan (SSP); February 2016; "Food and Agriculture Sector-Specific Plan, 2015"; UNCLASSIFIED; UNCLASSIFIED; The SSP details how the National Infrastructure Protection Plan (NIPP) risk management framework is implemented in the FA Sector, as developed through a coordinated effort between public and private sector partners. Available at https://www.dhs.gov/sites/default/files/publications/nipp-ssp-food-ag-2015-508.pdf.