Situational Awareness Report

September 28, 2022

Vermont Intelligence Center

VIC / HSEC SINs: 1 (Cyber)

(U) Cyber Threats to the Agriculture Sector

(U) Source: Google Images

(U) The food and agriculture sector has become an increasingly large target for cyber threat actors. These malicious actors can range from financially motivated cybercrime gangs to sophisticated nation-state hacking groups. The risk to the agriculture sector has also increased due to the expanding use of technology that is connected to the internet within the industry. Any device or piece of equipment with an internet connection is vulnerable to cyber-attacks. Often it is more an issue of when, and not if, cyber threat actors will target a critical device or valuable information. It is also due to the critical role that agriculture plays in local and national economies, as well as on the world market that has made it such a valuable target for threat actors. It is particularly critical for those involved in the agriculture industry to be aware of cyber threats leading up to and during harvesting season. Harvesting season often sees an increase in cyber attacks against the food and agriculture sector due to the impact that shutting down agricultural processes can have during harvesting. This can lead to global supply chain issues which have already been compounded by the Covid-19 pandemic and the conflict in Ukraine. **While the Vermont Intelligence Center is not aware of any specific threats to the agriculture sector in Vermont, it is important to be vigilant in protecting and mitigating cyber threats as harvesting season approaches.**

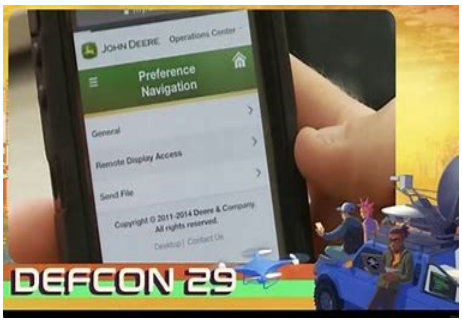
(U) Ransomware

(U) One of the largest threats to the agriculture sector is that of ransomware. Ransomware is a form of malicious software that encrypts data on a digital device. This can make affected systems completely inaccessible. The only way to unencrypt the data once it has been locked is to use a special key-code that will unencrypt the data. To receive the necessary key, the individuals who installed the ransomware will demand a ransom be paid. It has also become increasingly common that the threat actors behind ransomware attacks will first steal sensitive data from the victim and tell them that if they refuse to pay the ransom, not only will their data remain encrypted, but they will also leak their stolen data online. This tactic is referred to as double extortion. There have been many cases of large food and agriculture companies and, farms being impacted by ransomware. In 2021 a global meat processing company, JBS, had their operations shutdown by a ransomware attack.[1] Also in 2021, food cooperatives in the Midwest were targeted by Russia-based ransomware gangs. The attacks shut down the operations of NEW Cooperative, which provides feed, grain, fertilizer, and crop protection services to farms in Iowa, as well as the Crystal Valley Cooperative which services over 2,500 farms in Minnesota and Iowa.[1] A bit closer to home, in March of 2022 the Hood Dairy company was impacted by a large cyber incident believed to have been a ransomware attack. This shut down production in many of there facilities nationwide, including the Vermont based and Hood owned Booth Brothers facility in Barre. **While these are examples of attacks on large companies and cooperatives, the same threat exists for small local farms in small states like Vermont, and unfortunately there are many more examples of small farms having their operations shut down due to similar ransomware attacks.** Ransomware is particularly dangerous when used against the food and agriculture sector due to its disruptive nature. This is the most likely type of attack that will shut down the operations of farms and cooperatives. The affects of such attacks are not just financial for the farmers involved but can also prevent food and important products from getting where it needs to go. This can have a much larger impact on the economy and food supplies.

(U) Data Theft

(U) Source: Google Images

(U) Data theft is another threat that can have a large impact on the food and agriculture community. Technology has been increasingly implemented in farming operations to help increase productivity and crop yields. While this has had beneficial impacts, there are also threats involved. As previously mentioned, the devices and technologies used to operate a farm can be shut down through disruptive attacks such as ransomware. In addition, the technology used by farmers is often used to collect data. This data is often critical to farming and business operations and leaves farmers potentially vulnerable to data theft. Data theft is something that has become increasingly valuable to cyber criminals. There are entire networks of online marketplaces for cyber criminals to buy and sell valuable data. This data



is often critical to farming and business operations and leaves farmers potentially vulnerable to data theft. Data theft is something that has become increasingly valuable to cyber criminals. There are entire networks of online marketplaces for cyber criminals to buy and sell valuable data. This data can be used to carry out further attacks in the future, extort victims, or be sold to interested buyers seeking to exploit the stolen data. Essentially, the internet has provided a platform for massive data theft industries to flourish. The data used by farmers can include information on crop yields, herd health, land prices, and much more.[2] All of this is critical data to the business operations of a farm. To have data like this stolen and sold online can have not only a financial impact but an emotional one as well. What makes this security issue even more challenging is that much of the data collected by farmers will be protected and in the hands of third parties.[2] In many cases this is necessary, considering the amount of data collected it would be impossible for many farmers to store and protect that data on their own. The problem with third party data storage is that the security of a farmer's data is in the hands of someone else. The companies that store critical data for others often become targets for cyber criminals looking to exploit that data for financial gain. The platforms that have access to famers' data could include apps that are being used to operate farming technology, cloud services used to store data, and other similar services utilized in the agricultural industry.[2]

(U) Equipment Vulnerabilities

(U) Farming machinery has also been subject to increasing cybersecurity threats. These threats have affected large manufacturing companies such as AGCO, which was hit with a ransomware attack in May of 2022, but can also have much more direct impacts on local farmers. Tractors and other similar farming equipment is often now operated through software that controls the machine. Like other advancements in farming technology, this leaves it vulnerable to being hijacked by cyber threat actors. Companies, such as John Deere, often have ownership over the software that their machines run on. This effectively means that John Deere networks control the equipment used by farmers all over the country to conduct their business.[3] The vulnerabilities to networks like this have recently been exposed in a number of situations. An example of this would be when just last year, in 2021, a group of penetration testers were able to hack into John Deere's Operations Center in less than 48 hours. By gaining access to the Operations Center, they effectively could control equipment on any farm connected to those John Deere computer networks. This gave the penetration testers access to the farmers' data, irrigation systems, and water supplies.[1] Luckily, this discovery was made by penetration testers, who are paid to test the cyber defenses of different companies. If it had been a malicious actor who had done the same thing, the impacts could have been much more serious. The same type of risk applies to the software used to control tractors and farming equipment. This was highlighted at this year's DEF CON cybersecurity conference, in which a penetration tester showcased how he was able to take control of a console used to operate a John Deere tractor.[3] John Deere also has further planned to connect more machines to its online cloud service network. These events have called into question the security of the networks and software controlling farming equipment. If a malicious actor were able to access the networks controlling tractors nation-wide, they could unleash a devastating attack that could potentially physically shut down tractors during harvesting season and cause massive disruptions to farmers' abilities to harvest. It should be noted however, that while there is a risk of something like this happening an attack of that type has not yet been achieved.

(U) These threats are merely examples of different types of attacks that can occur against the agriculture sector. **The underlying idea to these threats is that, as with other industries, farming and agriculture has become more reliant on technology and therefore more vulnerable to cyber threats.** This is not inherently a bad thing; other industries have adapted well to the risks that come with implementing more technology and becoming more digitally connected. The agriculture sector must take similar steps to increase security, mainly because of how critical this industry is to society. Many of these security measures must be implemented by larger companies within the agriculture sector such as cloud service companies and manufacturers. There are, however, things that local entities and farmers in the State of Vermont can do to improve their security.

(U) Below is a list of mitigations that will help to enhance cyber resilience.

- Create an inventory of the digital devices and equipment that enable business operations.[4]
- Assess those systems' security controls and how vulnerable they may be (this may require cybersecurity professionals with technical training).[4]
- Regularly back up data and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Implement network segmentation.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, the cloud).
- Establish, test, and update incident response and continuity of operations plans.
- Install updates/patch operating systems, software, and firmware as soon as they are released.
- Use multi-factor authentication (MFA) where possible.
- Use strong passwords - regularly change passwords to network systems and accounts, implementing the shortest acceptable timeframe for password changes. Avoid reusing passwords for multiple accounts.
- Disable unused remote access (remote access protocol ports) and monitor remote access logs.
- Require administrator credentials to install software.
- Follow the principle of least privilege and audit user accounts with administrative privileges.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a VPN.
- Consider adding an email banner to messages originating outside your organization.
- Disable hyperlinks in received emails.
- Focus on cyber security awareness and training. Regularly provide users with training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities (i.e. ransomware and phishing scams).[1]
- Contact the Cybersecurity and Infrastructure Security Agency (CISA). CISA has many resources available to help organizations build their cyber resiliency. Homepage | CISA

(U) For any further questions or concerns related to cybersecurity threats to the agriculture sector in Vermont, please reach out to Ryan McLiverty, the Cybersecurity Analyst at the Vermont Intelligence Center. He can be reached via email at ryan.mcliverty@vermont.gov or by phone at 802-371-9954.

(U) Contact the VIC for a list of sources at dps.viccyber@vermont.gov.