Seeds'N'More is an organization in the Agricultural Industry in the United States. They are based out Southern Indiana and produce and sell seeds, such as corn, wheat, soybeans, hay, and tomatoes, while also importing and selling other seed crops not commonly found in Indiana. As well as grow and sell harvested crops in the United States. They do ship seeds internationally, but do not ship crops internationally. There current are 3,000 employees working for Seeds'N'More and their revenue each year has averaged to be about $300 million dollars.

They most recently have merged through the buy-out of a major competitor also in the Southern Indiana area. The merge is estimated to bring $200 million in new revenue (about $500 million in yearly revenue). Also, with the merge hey have just added 2,000 new employees into their systems. Seeds’N’More as also implemented a new Enterprise Resource Planning System and have been working on their use of the Internet of Things to make their business more efficient.

The ERP system that Seeds’N’More has just implemented is cloud based and is accessed through any browser. They primarily use Gmail for communications purposes, and all employees are required to change their email password every 3 months and meet the CIO’s standards of length and sophistication to ensure a higher level of security. Employees are also not allowed to open personal email at their work station or on the main network. They are allowed to use the break buildings network to do so on their break or during their lunch hour. The break buildings network is kept completely separate from the main network and sub networks. They do have a Virtual Private Network setup for remote login capabilities and it is monitored very carefully. Their IT department monitors for unusual traffic on non-standard ports and closed all unused ports.

The largest security risk that I believe that their network may face is that dealing with protecting their crops and their use of the Internet of Things. Seeds’N’More is currently using IoT devices to monitor water levels in soils and soil health and components. They are also using drones that can detect weeds and spray them with weed killer. All of the results, data, and controls are located in on site servers on the Agri-department network, which is a sub network of the Main building network. Other large security threats include the data they collect on their fields and crops, as well as susceptibility to ransomware attacks.

The types of information that Seeds’N’More has that contain value include their crop and field data, drone capabilities and control, seed manufacturing data, and order data. With field data, some of the projection and information is based off of national data, if that data is corrupted, false, or hacked, the entire agricultural market would be severely crippled (FBI). It could potentially cost Seeds’N’More up to 75 percent of their business, in this case $375 Million. If their crops do not thrive by at least a 65% margin (they set it up this way to account for bad years etc.) then the business as a whole suffers greatly. They also do have some seed business to help offset but most of the seeds they sell come from the crops they grow.

With the drone control, operations, and data it is also has quite a value. Seeds’N’More if they were to lose control or get sabotaged by a competitor then they could lose a large majority if not all of their crops due to the drone spraying and killing the crops instead of weeds. Again, I think that this information would also be worth about $375 Million. If tampering or sabotage were to happen with the manufacturing of seeds, believe that this would be less detrimental to the business. I believe that this would affect 25 percent of the revenue which amounts to $125 Million. In this case that is still quite a bit but not as much as the crops side. Order/contract data could also be stolen or be a part of a ransomware attack. Seeds’N’More has many procedures put into place so that the likelihood of such an attack happening would lessen, but it could still happen. Depending on the demands, I think that it would be reasonable for Seeds’N’More to pay a ransom, but not multiple. Also, after the attack reevaluations should be made in procedures and security testing, employee awareness, and employee training should be conducted to prevent further attacks.

Customers personal information is also of some value. I estimate this to be among the greatest losses in the long run for Seeds’N’More. If their customers information is stolen and used then Seeds’N’More would lose a large percentage of their business. Whereas if crops or seeds were damaged we could potentially gain customers back, but with the loss of personal information it is nearly impossible to gain back the trust of customers. I estimate that if a breach of personal information is made that Seeds’N’More would probably lose 50 percent of their customer base ($250 Million).

In conclusion, for Seeds’N’More, I believe that for the capabilities of sabotage that crop data, drone control, and seed manufacturing would be the areas to strike for an attacker. On the aspect of money or profit for the attacker, ransomware or customers personal information (payment info) would be the most profitable areas to strike. These are the areas that Seeds’N’More needs to continue to build up protection against.

Works Cited

*Cybersecurity in the Agrifood Sector*. www.wur.nl/upload\_mm/4/6/a/f74a893e-c829-4bf3-9884-e357929ff5d6\_Cybersecurity%20in%20the%20agrifood%20sector.pdf.

“Agriculture, Farming, Cyber Attacks | Homeland Security Newswire.” *Gait Biometrics Shows Promise | Homeland Security Newswire*, 2015, www.homelandsecuritynewswire.com/dr20150220-u-s-farming-sector-increasingly-vulnerable-to-cyberattacks.

Bedord, Laurie. “Midwest Agriculture Is a Prime Target for Theft of Intellectual Property and Cyber Attacks.” *Successful Farming*, Successful Farming, 5 Apr. 2016, www.agriculture.com/content/cybersecurity-is-not-just-a-big-city-problem.

Cheh, Samantha. “Agriculture Is Our Most Vital Industry and It Needs Cybersecurity.” *Tech Wire Asia*, 28 Dec. 2017, techwireasia.com/2017/12/agriculture-iot-needs-more-cybersecurity/.

“FBI Warns Agricultural Industry about Increasing Cyber Risk.” *Cline Wood*, 21 Nov. 2017, clinewood.com/2017/10/11/fbi-warns-agricultural-industry-increasing-cyber-risk/.

“Phishing Attacks in the Agriculture Industry.” *InfoSec Resources*, resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/phishing-attacks-by-demographic/phishing-attacks-in-the-agriculture-industry/.