EXECUTIVE MASTER IN CYBERSECURITY

PRECISION AGRICULTURE AND AGTECH:

AN INDUSTRY RISK ASSESSMENT

Megan K. Schatzman

Brown University, Executive Master in Cybersecurity (EMCS)

Critical Challenge Project

February 24, 2019

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In recent years global agriculture has faced adversity; with trials including climate change, water scarcity, loss of arable land, and even workforce shortages. Amidst this reduction in resources, populations across the globe continue to rise. Increasing the demand for food production. Precision Agriculture was borne out of a need to do more with less, and refers to the application of advanced technologies to farming with the ultimate goal of increasing crop efficiency. AgTech became an umbrella term for all Food and Agriculture applications of technology, and has become an industry in its own right.

The Food and Agriculture sector has been recognized by the United States Department of Homeland Security (DHS) as a critical infrastructure representing over 2 million American farms and accounting for roughly one fifth of the nation's economic activity. [1] With the rapid increase of technology on farms and the increasingly connected nature of devices, risk of cyber attack on the nation's food supply is higher than ever before. The US is merely one example of a nation whose Food and Ag industry is potentially vulnerable to this brand of attack.

The purpose of this critical challenge project is to explore potential threat vectors introduced through the rise of AgTech and Precision Agriculture. In the absence of a cybersecurity risk framework specific to this industry, this paper proposes a matrix to categorize risks by criticality.

> *"These threats are not trivial. Whereas an industrial-scale cyber-attack in any industry can do significant harm to a business's bottom line, such an attack in the agricultural sector could see whole crops decimated and have severe consequences for the quality of life of entire populations." [2]*
>
> *- Chris Harry-Thomas*
> *Director of Sector Development Agriculture, Inmarsat Enterprise*

INTRODUCTION

In the several million years that humans and early humans have roamed this earth, we have undertaken three widely recognized agricultural revolutions. References to a fourth agricultural revolution have now begun cropping up anywhere from content sharing platforms like Medium to leading sector conferences. In his address at the 2019 Oxford Farming Conference, UK Secretary of State for Environment, Food and Rural Affairs Michael Gove stated in no uncertain terms "as this conference is designed to underline, our world is entering a fourth agricultural revolution". He further went on to state, "[this revolution] will force us to reform the role of government in regulating and supporting farming". [3]

The nature of regulation Gove is referring to would be tasked to increase adoption of precision agriculture technologies in order to guarantee the United Kingdom's future as a "major, global food producer". The position comes as no surprise at a time when 20% of British farms are failing to turn a profit. [4] He describes the future he envisions for Britain, highlighting a technology-enabled symbiotic relationship with the earth.

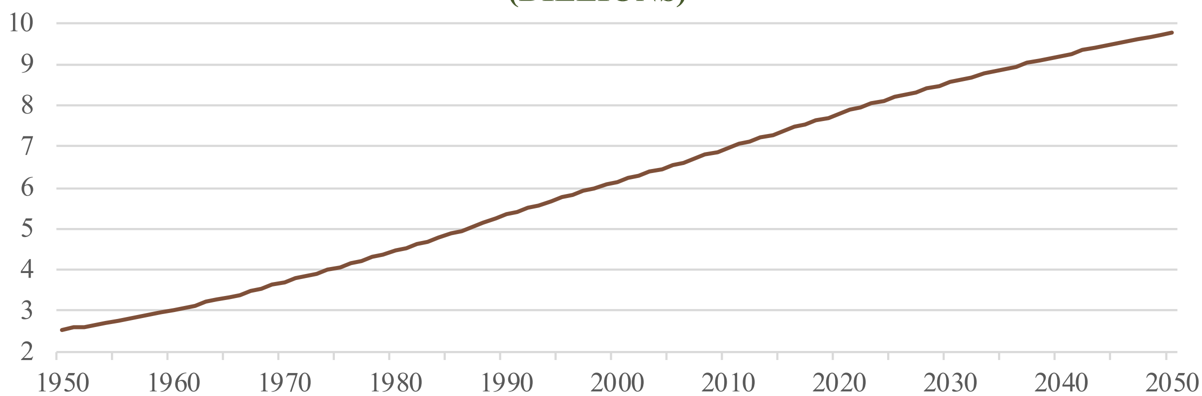
The UK is not the only country in this race to feed a growing population with the impacts of worsening climate change looming over them. The incentives to increase AgTech adoption become clear through careful inquiry of the current state of affairs in agriculture globally.

STATE OF GLOBAL AGRICULTURE

FEEDING THE GROWING POPULATION

Population growth is expected to increase by 33% to nearly 9.8 billion by 2050 (from 7.6 B). [5] Increasing population will mean increasing demands for food, a concerning trend when much of the world's needs are already not being met. The United Nations Food and Agriculture Organization (FAO) estimated that in 2017, 820 million people faced chronic hunger. This staggering figure is just under 11% of the world population. Food scarcity is also a driver in increased obesity rates with lack of access to fresh natural foods serving as a contributing factor of obesity. [6] The challenge is to not only feed the masses, but to feed them well. Placing agriculture directly at the center of this great undertaking.

ACTUAL AND PROJECTED WORLD POPULATION SIZE (BILLIONS)



POPULATION DATA PROVIDED BY UNITED NATIONS DEPARTMENT OF ECONOMIC AND SOCIAL AFFAIRS [7]

The rise in population alone translates to less arable land per capita, coupled with the loss and degradation of available farmland seen by many nations in recent years, the impact is compounding. Most of the globe appears to be affected by the reduction of arable land per capita.

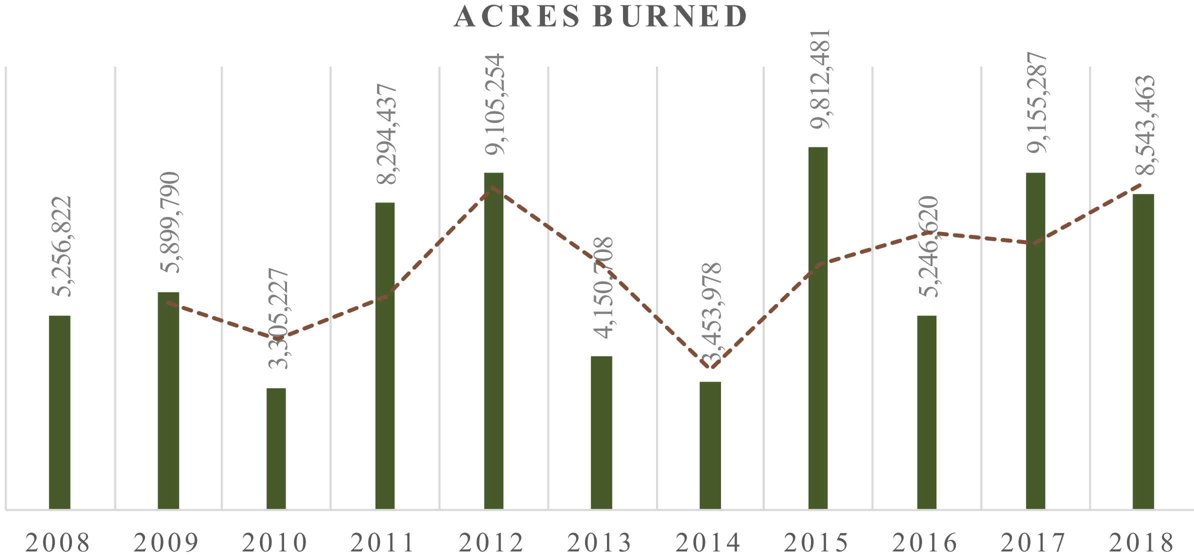
For some countries the decreases have been particularly dramatic in the last 20 years. Including the United States, Niger, Russia, Mongolia, and New Zealand. [8]

ENVIRONMENTAL FACTORS CREATING INHOSPITABLE GROWING ENVIRONMENTS

The planet has lost one third of its arable land in the 40 years leading up to 2015. [9] Of what remains, 25 percent of all farmland globally is already rated as highly degraded, with another 44 percent rated as moderately or slightly degraded. [6] The degradation of our farmland has a myriad of causes including water scarcity, and natural disasters. The loss of arable land in general includes the aforementioned with the addition of non-climate driven causes like settlement of the land. Water scarcity is most prevalent in the Middle East and North Africa (MENA), but is also high risk in the Western portion of the United States, as well as Argentina, United Kingdom, and China. [10]

Frequency and intensity of natural disasters is on the rise globally, with major storms, flooding, droughts and extreme temperatures dominating news headlines. [11] Many of these natural disasters create inhospitable growing conditions, for example by drowning or drying crops. One natural disaster has taken center stage in the last decade as dry conditions incite more widespread damage, wildfires.

Wildfires have the potential to cause devasting impact to farmers, not only due to the crops and facilities that are burned in the blaze but additionally to future crops through the lasting damage to the soil at the sites of these fires. While there are no figures released on acreage of general farmland lost to wildfires, an alarming 8,582,609 acres of land were burned in the US alone in 2018. [12]



WILDFIRE DATA PROVIDED BY NATIONAL INTERAGENCY FIRE CENTER – UPDATED NOVEMBER 2018 [12]

One such crop to be heavily impacted was the marijuana industry in the State of California, where wildfires have been particularly prevalent. The growing of marijuana was legalized on the basis of providing considerable tax revenue for California's counties. In 2017, Sonoma county had estimated that by mid-2018 they would generate $3.8 million in tax revenue from the cannabis industry. Unfortunately for Sonoma, Fall of 2017 brought devastating fires leaving many growers with significant losses and the county woefully short of their promised tax revenue. [13] The California Growers Association estimated that between 30 and 40 percent of cannabis growers in the state were impacted by wildfires in that year. [14]

CLASSIFYING FOOD INSECURITY

Headquartered in Rome, the Food and Agriculture Organization (FAO) of the United Nations was established with the intrepid goal of working with organizations, individuals, and governments to end world hunger. Their work includes researching the global prevalence and impact of malnutrition, as well as monitoring the pervasiveness of food and water scarcity. In order to categorize these, the FAO has devised and leverages outside indexes reminiscent of the makings of a risk framework. Among these indexes the FAO rates food insecurity on the four dimensions of Availability, Access, Utilization, and Stability. [15] Utilization in this instance refers generally to food waste or over production. In order to classify the severity of a nation or region's food insecurity, the FAO uses the Integrated Food Security Phase Classification (IPC).

IPC PHASE CLASSIFICATION
Generally food secure
Chronically food insecure
Acute food and livelihood crisis
Humanitarian emergency
Famine/humanitarian catastrophe

UN FAO: FOOD SECURITY INFORMATION FOR ACTION [15]

Through these guidelines, food insecurity can also be broken down by length or interval of the shortage or availability constraints.

TYPES OF FOOD INSECURITY

Chronic	long term, persistent
Transitory	short term, temporary
Seasonal	predictable, sequential

UN FAO: FOOD SECURITY INFORMATION FOR ACTION [15]

FARM LABOR SHORTAGES

In 2018 portions of Scottish fruit crops were rotting in the fields after a 10 – 20% workforce shortage meant produce was ripening faster than it could be picked with the available labor. [16] In light of an already constrained workforce, fears are running high in the United Kingdom as Brexit threatens the stability of the Britain's farm labor force. The United Kingdom has plans to trial a seasonal visa for non-EU farm labor from 2019 through 2020. [17] Australian Federal Agriculture Minister, David Littleproud, has stated the government may be moving forward with a new category of visa to allow migrants to come to Australia legally without prior sponsorship and take up jobs in agriculture. [18] American farm bureaus have been lobbying for similar visas to be made available in the United States in order to address the same labor challenges. [19] With farm labor constraints being felt across the globe, nations will be competing to attract the limited workforce into their borders.

TECHNOLOGICAL SOLUTIONS TO AGRICULTURAL CHALLENGES

Agricultural Innovation ranges broadly from advanced drone technology surveilling crops, to the humble "pomato" – a tomato plant spliced onto a potato root system, thereby increasing yield for both produce. The strain to do more with less has given rise to crop-saving agricultural technologies, as well as a booming new market sector.

Once a great agricultural innovation on their own, greenhouses have been in use since the 1800s. Enabling farmers to grow at all times of year, in any climate. Today greenhouses have become a sophisticated, connected environment. Boasting innovative climate control systems, automated shades to regulate the intake of sunlight, and advanced irrigation systems.

Irrigation has also seen noteworthy new developments in recent years, systems are now capable of monitoring the status of crops in both fields and greenhouses, and stragically watering only where and when that water is needed. Unlike timed irrigation systems, which were once a tremendous leap forward, these are able to make decisions about water needs. For example, not watering crops after a rainstorm. To achieve this, these systems rely on technologies such as IoT sensors to provide information about the health and water content of the soil. They are also able to leverage machine learning algorithms to maximize the utility of water used. Some systems even receive their data from drones which surveil the crops overhead and communicate down to the irrigation systems where water is needed.

Drone technology is capable of even more impressive feats than communicating with irrigation alone. Agricultural drones leverage near-infared and multispectral cameras to assess crop health from overhead. These specialized cameras are adept at identifying and pinpointing the location and severity of outbreaks of pests and disease. They can also provide rich data about soil health, and alert to when fertilizer or a crop rotation is needed. Their abilitiy to carry a payload and communicate with decision support systems enables these drones to deliver resources to where they are needed most; such as feed or insecticides. Using thermal imaging, drones can also locate livestock, even in the dark. Drones on farms also have some more traditional uses, such as allowing the pilot to easily inspect roofs of greenhouses, barns and outbuildings. Traditional methods of insepcting roofs can be dangerous to inviduals and require more time and care to perform.

As pictured on the left, only a limited portion of this roof can support the individual inspecting it, limiting their view of all areas of the roof. A drone is capable of providing visibility into areas a person simply cannot reach.

Some of the most remarkable new agricultural technologies are autonomous equipment and vehicles. These include unmanned and fully autonoous tractors, such as those pioneered by John Deere. Which unlike other self-driving vehicles are able to go to market quickly with minimal regulatory hurtles as they are operating on private land rather than public roadways. These vehicles can plant, plow, harvest, distribute pesticides and more with stunning accuracy. [20]

Control systems, drones, and autonous vehicles alike are a few of many types of conntected devices present in agriculture. Internet of Things (IoT) devices are used in numerous applications to support AgTech. Livestock can be monitored by connected tags in a wireless mesh. Soil probes monitor and report on soil health, including attributes like water saturation and pH balance. Sensors in silos monitor the available grain, along with many more devices and applications. [21]

By tapping into the rich data connected on the network of connected devices, machine learning has seemingly limitless applications in the agricultural sector. Within permaculture, machine learning is being used to predict algae blooms. On livestock farms, genetic algorithms selectively breed cattle for specific traits. Machine learning is being used across the industry to predict yield and harvest time, maximize water and resource efficiency, detect diseases in plants, and monitor the health of animals. [22]

These algorithms also help to support gene editing and genetically modified organism (GMO) development. CRISPR targeted genome editing can help protect native species against the effects of climate change, increase the yield of crops, foster disease resistance in plants and animals, and even increase the nutritional value of food products. [23]

SECURITY RISKS AND THREATS TO PRECISION FARMING

Revisiting the FAO's categories of food insecurity; Availability, Access, Utilization, and Stability. Three of these four have clear links back to cybersecurity. With availability and access representing Availability on the CIA Triad, and stability representing Integrity.

THREAT ACTORS AND BODIES OF RISK

Agriculture could be targeted by hacktivists, state sponsored actors, competition, disgruntled current and former employees, and financially motivated actors. The industry also faces non-targeted threats such as natural disaster, advanced persistent threats (APTs), and regulatory risk.

Hacktivism is where activism and cyberattacks converge, one particularly well known group of self-proclaimed hacktivists is Anonymous. The group is known for carrying out distributed denial of service (DDoS) attacks against organizations and governments on the grounds of social activism. [24] Anonymous associated videos have appeared online condemning GMOs and urging others to take action. Agricultural industries rely heavily on genetically modified crops to succeed on a resource strapped planet. With the group's history of delivering on such attacks and the focus and growing public concern over GMOs, the risk of hacktivism is mounting in the industry.

Critical Infrastructure stands at the center of cyber warfare, in the United Kingdom more than 10 cyberattacks on critical infrastructure weekly rose to the level of NCSC (National Cyber Security Centre) involvement. [25] Given the increasingly digital nature of warfare, governments should anticipate cyberattacks on critical industries as a potential threat vector for state sponsored attacks.

Competition and insider threats are far from specific to the Food and Agriculture sector, however a growing presence of connected technologies in farming is increasing the threat vector. This rise in technology is also opening the door to risk from APTs such as ransomware which could now impact anything from a greenhouse control system to farming equipment.

The regulatory environment is favoring better privacy protections for data subjects necessitating organizations to strengthen their data security and privacy posture, agriculture will be no exception.

DATA PRIVACY AND SECURITY

As is the case in most industries, agricultural businesses are vulnerable to unauthorized use and disclosure of personal data (PII), as well as business critical data and intellectual property (IP). To address this growing risk, six European agricultural organizations and associations banded together with the assistance of the EU commission to publish a voluntary EU Code of conduct on agricultural data sharing. Types of sensitive data a farm may produce includes but is not limited to agronomic data, genetic data on livestock, machine data, plant patents, GIS data and PII. [26]

Agronomic data is unique to the farm where it was produced and includes information like yield data, pesticide use, and soil data. This data is inimitable in that it is not easily transferrable from one farm to the next. It generally accounts for factors like weather conditions and soil type. [27] It would seem on the offset that leakage of agronomic data would be inconsequential to the farm where it was collector. However, this data reveals the unique mix that enables the business to produce. This type of information in malicious hands could be vital intel if the attacker's intent was to sabotage operations.

Genetic algorithms for the purpose of selective breeding is yet another industry specific category of data that agricultural businesses should protect. Competition is decidedly fierce in an industry where selectively bred animals fetch enormous sums of money at auction. One such animal, a ram called "Texel Tophill Joe", fetched £128,000 in 2003. He in turn sired lambs that earned his purchasers £1 million. Just three years after the sale of Tophill Joe another Texel set a record by selling for a staggering £231,000. [28] Understanding the profits breeders stand to gain helps shed light on why an attacker would be incentivized to steal such data. Another reason for selective breeding is for the health and wellbeing of livestock, an adversary may want to tamper with such algorithms in order to cause a rival farm to breed for the wrong traits, resulting in an unhealthy generation of animals. [29]

As with all industries, Personal Data is protected in certain jurisdictions and will open organizations collecting this data category to regulatory risk. The most notable regulation in this space is the General Data Protection Regulation (GDPR), which mandates protections on the privacy of personal data regarding EU data subjects.

TAMPERING WITH CONTROL SYSTEMS

In 2015 over 300,000 chickens were killed in a targeted attack in South Carolina, when a suspected disgruntled former employee of a poultry farm tampered with climate controls on several farms in Bishopville. The attacker strategically turned off alarms systems before overheating the houses, suffocating the chickens overnight. The resulting losses from this attack amassed an estimated $1.7 million. [30] The attack was carried out with intimate knowledge of the control system peripherals and required physical access to the houses, which was achieved under the cover of night. While rudimentary as an attack, a farm employing connected control systems could see an attack of this nature achieved at a massive scale with little prior knowledge or physical access required. Particularly in instances where a relatively rudimentary control system is exposed to the internet. Even in circumstances where control systems are complex, such as in the case of machine learning algorithms, adversarial attacks could cause bad predictions or behaviors to malnourish, overfeed, or kill crops and livestock.

NETWORK AND IOT ATTACKS

Disruption of IoT sensors and networks could impact the confidentiality, integrity, and availability of the AgTech applications outlined above including irrigation systems, autonomous vehicles and equipment, and climate control systems. Connected devices pose threat of exposure to APTs such as ransomware attacks. Improperly configured control systems could leave access to industrial controls open to the internet. IoT devices could be leveraged as thingbots, botnets specific to connected devices. Man in the Middle (MitM) attacks could cause sensitive data to be improperly issued or disclosed. Disruption of Position Navigation and Timing (PNT) systems, such as GPS, could misdirect drones, autonomous vehicles and misrepresent GIS data regarding crop statistics and health. [31]

A 2002 study conducted in the United States found that fruits and vegetables traveled approximately 1,500 miles on average before being sold to the end consumer. [32] The FDA estimates that 15% of the nation's food supply is imported. [33] Disruption of supply chain both domestic and international could cause catastrophe impacts on the United States Food and Ag supply chain. Attacks on shipping and shipping ports have been realized in the past and can have a ripple effect through many industries.

CASE STUDY: MAERSK RANSOMWARE ATTACK 2017

In the Summer of 2017, a NotPetya ransomware attack (one form of APT) impacted the shipping conglomerate Maersk. The exploit preyed on unpatched servers and severely impacted the company's shipping capabilities for 10 days. In total, their losses are estimated to be $300 million –harming not only the organization but the downstream supply chain as well. [34]

With an estimated 15% of America's food supply being shipped from beyond US borders, there is a high level dependency on this supply chain. In other nations, such as the United Arab Emirates, limited natural resources necessary for food production increase dependence on imports to critical levels. It is estimated that up to 85% of the UAE's food supply is imported. [35]

CASE STUDY: SUPERMICRO CHIPS 2014

In 2014 China successfully compromised major US tech companies by infiltrating the supply chain and inserting microchips into hardware bound for server company Supermicro that supplied tech giants and even the United States government. [36]

With the prevalence of drone manufacturing in China, such an attack could easily be realized on drones bound for US farms. Concerning motivations of a nation state from a confidentiality risk perspective would include exfiltration of aerial imaging of critical infrastructure, trade secrets and non-public information, and agronomic data. [31] From an integrity risk standpoint, altering positioning systems could cause water, feed and pesticides to be misdirected – harming crop health potentially killing crops if gone undetected. Tampering with multispectral, infrared and near-infrared cameras could prevent disease or poor health from being detected while further attacks are carried out.

MARKET RISK

Particularly in nations such as the United States, where agriculture accounts for nearly 20% of economic activity, catastrophic events to agriculture would undoubtedly lead to critical market impact as well. [37] As is the nature of critical infrastructures, they are also interdependent on one another. Dramatic impacts to the fuel arm of agriculture in the United States would have an impact on the energy sector, as Diesel fuel is a sizable output of American agricultural crops. Public disclosure of non-public information could be a weapon for competition and nation states to disrupt trade in markets which could cause detrimental impact to agricultural sectors or national economies. [31]

PHYSICAL SECURITY

Farms are uniquely challenged as it relates to physical security, it can be disproportionately expensive or impossible secure physical assets and equipment. For many, the risk of theft or destruction is worthwhile tradeoff over attempting to front the cost of physical security solutions.

There is no evidence to suggest that the rise of AgTech has prompted a shift in this risk posture at this time, though it appears unlikely that an increase vulnerable assets could change the circumstances in which is it simply difficult to protect equipment on expansive and open land. The large and open nature of farms add a layer of vulnerability to the connected technologies being deployed.

SECURITY SOLUTIONS FOR AGRICULTURAL CHALLENGES

Not all security developments spell gloom for AgTech, some cybersecurity advancements show promise in solving industry problems both old and new. One such technology with seemingly limitless applications in the industry is Blockchain.

Blockchain technology can aid in pinpointing the source of outbreaks of disease or contamination, and trace contaminated food through the supply chain, enabling efficient and targeted recalls to a level of precision never previously realized. The technology may also help to build trust in food labeling particularly for Fair Trade and ethically sourced commodities, such as coffee. [38]

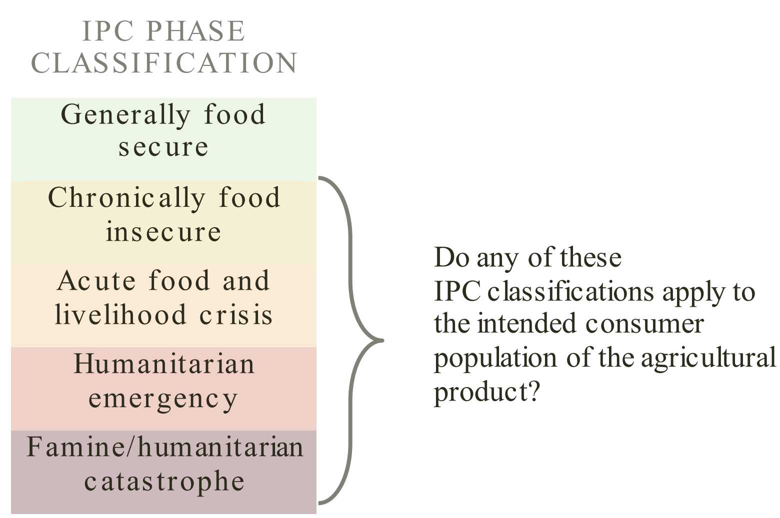
Cryptographic protocols may offer protections for sensitive data types collected in the field. Encryption applications may also provide solutions for non-technical challenges in agriculture. Zero knowledge proofs may, for example, present a viable solution to anonymous crop testing.

PROPOSED RISK MATRIX FOR ASSESSING AGRICULTURAL TECHNOLOGY THREATS

There is no chart or formula that is designed to quantify impact or likelihood of cyberattacks in the Agricultural sector, as such it is at the discretion of the organization to do appropriate due diligence to rank with some degree of confidence the expected level of impact that may be realized in the event of an attack on any AgTech or Precision Technology product or service. Furthermore, to assess how likely that risk is to be realized. Included below are sample questions to ask yourself, your peers, and your organization to assist in formulating an impact and likelihood score. These principles have been adapted from NIST Guidance for Conducting Risk Assessments. [39]

EVALUATING IMPACT

- What is the market risk? Would an attack on the Confidentiality, Integrity, or Availability of this product or service negatively impact financial markets in a measurable way?
- What is the level of food security for the target market? Refer to the IPC Phase Classification reiterated below.



- Could the impact of an attack be costly to organization? More than the cost of the product or service itself?
- How might a breach of data from this system impact the organization or the data subjects?

- Is there potential to harm shareholder value?
- Could an attack or breach pose regulatory risk? Consider, for example, privacy regulations.

CLASSIFYING IMPACT

Using the questions and considerations above, along with any other considerations pertinent to your organization, you can classify the potential impact as Low, Medium, High, or Critical.

LOW IMPACT	○ Low, negligible, or no financial losses ○ Minimal or no disruption to operations
MEDIUM IMPACT	○ Moderate financial losses ○ Hindered operations
HIGH IMPACT	○ Significant financial losses ○ Halted or severely impeded ability to do business
CRITICAL IMPACT	○ Devastating financial losses ○ Poses risk to human health or human life ○ Risk of harm to another critical infrastructure

EVALUATING LIKELIHOOD

- Is physical access control attainable for this solution?
- Consider how other compensating controls protect this asset.

- What motivations may exist to attack an asset of this kind? Consider financial, activism, and other motivations discussed previously in this paper.
- Consider natural events that might have a negative impact on this asset, such as solar flares and natural disasters.
- Would it require a significant amount of institutional knowledge to perform such an attack?
- Would the cost of such an attack be equal to or more than what the attacker would stand to gain?

CLASSIFYING LIKELIHOOD

Using the questions and considerations above, along with any other considerations pertinent to your organization, you can classify the potential likelihood as Low, Medium, or High.

LOW LIKELIHOOD	Risk realization is feasible, yet unlikely to occur
MEDIUM LIKELIHOOD	Risk realization may occur at some point
HIGH LIKELIHOOD	Risk realization will likely, or is expected to, occur

CATEGORIZING RISK EXPOSURE

Based on your evaluation of impact and likelihood, you can determine the overall risk of adopting an AgTech product or service using the matrix below.

		LIKELIHOOD		
		Low	Medium	High
IMPACT	Low	Risk Level 5	Risk Level 4	Risk Level 3
	Medium	Risk Level 4	Risk Level 3	Risk Level 2
	High	Risk Level 3	Risk Level 2	Risk Level 1
	Critical	Risk Level 2	Risk Level 1	Risk Level 0

Organizations may choose to break down their risk scores independently by category, for example by leveraging the CIA triad as shown below, or across the FAO categories of Availability, Access, Utilization, and Stability.

	RISK LEVEL					
Confidentiality	5	**4**	3	2	1	0
Integrity	5	4	3	**2**	1	0
Availability	**5**	4	3	2	1	0

GUIDANCE FOR INTERPRETING RISK SCORES

RISK LEVEL 0	Do not proceed
RISK LEVEL 1	Proceeding with this solution is not advised If solution deemed essential - proceed with extreme caution Have a business continuity and/or disaster recovery plan in place
RISK LEVEL 2	Proceed with caution Have strong compensating controls in place Have a business continuity and/or disaster recovery plan in place
RISK LEVEL 3	Proceed with caution Identify opportunities for compensating controls Have a business continuity and/or disaster recovery plan in place
RISK LEVEL 4	Proceed Where deemed necessary, have recovery or continuity plans in place
RISK LEVEL 5	Proceed

RECOMMENDATIONS

BUILDING PUBLIC – PRIVATE PARTNERSHIPS

A critical first step towards addressing this emerging threat landscape is through awareness and education. For the development of threat intelligence in this industry to be most effective, both public and private sector bodies will need to come to the table. One possible starting point to this relationship is by reinstating the Food and Ag Information Sharing and Analysis Center (ISAC) in the United States.

INTERNATIONAL COOPERATION

The threats laid out in this paper are global and interconnected, it is in all nation's best interest to ensure the sustainable cultivation of food for our future. International Computer Security Incident Response Teams (CSIRTs) would be a long term goal of cooperation on cybersecurity risk to the food and agriculture sector. In the short term, the formation of multi-country ISACs and Information Exchanges can facilitate research and awareness of these threats. As an industry we must urge governments not to wait for the first humanitarian crisis to address these risks to Food and Agriculture.

REGULATORY CONSIDERATIONS IN THE UNITED STATES

In the United States, the Presidential Policy Directive (PPD) defines a critical infrastructure as:

> *"...the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a*

debilitating effect on security, national economic security, national public health or safety, or any combination thereof" [40]

Today the only regulatory oversight in the Food and Ag sector, one of 16 US designated critical infrastructure sector, is exercised through the Food and Drug Administration (FDA). [37] In some cases, governance and oversight also comes from the Centers for Disease Control and Prevention (CDC), such as in the event of a E. coli outbreak.

Research conducted for this critical challenge project did not produce any findings on what the impact of regulation could mean for Food and Ag. Preliminary research brings to light risk considerations with regards to extreme resourcing and knowledge constraints within the sector which could impede actionable regulation. A secondary risk is that regulation could bring unintended consequences to agriculture, and in particular food production, which could hinder adequate supply of goods. The recommendation with regards to regulation is that more research could be done in this area.

WORKS CITED

[1] United States Department of Homeland Security, "Food and Agriculture Sector," [Online]. Available: https://www.dhs.gov/cisa/food-and-agriculture-sector.

[2] Inmarstat, "Agritech in race to protect farmers from cyber threats," 14 December 2017. [Online]. Available: https://www.inmarsat.com/news/agritech-in-race-to-protect-farmers-from-cyber-threats/.

[3] Oxford Farming Conference, "Michael Gove MP Speaking at OFC," 2019. [Online]. Available: https://www.ofc.org.uk/video/michael-gove-mp.

[4] United Kingdom National Statistics, "Agriculture in the United Kingdom," 2018. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/741062/AUK-2017-18sep18.pdf.

[5] United Nations Department of Economic and Social Affairs, "World population projected to reach 9.8 billion in 2050, and 11.2 billion in 2100," 21 June 2017. [Online]. Available: https://www.un.org/development/desa/en/news/population/world-population-prospects-2017.html.

[6] United Nations Food and Agriculture Organization, "2018 State of Food Security and Nutition in the World," [Online]. Available: http://www.fao.org/state-of-food-security-nutrition/en/.

[7] United Nations DESA Population Division, "World Population Prospects 2017," [Online]. Available: https://population.un.org/wpp/DataQuery/.

[8] World Bank Open Data, "Arable land (hectares per person)," [Online]. Available: https://data.worldbank.org/indicator/AG.LND.ARBL.HA.PC.

[9] O. Milman, "Earth has lost a third of arable land in past 40 years, scientists say," 2 December 2015. [Online]. Available: https://www.theguardian.com/environment/2015/dec/02/arable-land-soil-food-security-shortage.

[10] World Resources Insitute, "Water Stress by Country," December 2013. [Online]. Available: https://www.wri.org/resources/charts-graphs/water-stress-country.

[11] The Economist, "Weather-related disasters are increasing," 29 August 2017. [Online]. Available: https://www.economist.com/graphic-detail/2017/08/29/weather-related-disasters-are-increasing.

[12] "National Interagency Fire Center," 2018. [Online]. Available: https://www.nifc.gov/index.html.

[13] The Press Democrat, " Fires destroy Sonoma County marijuana crop; millions in taxes at risk," 19 October 2017. [Online]. Available: https://www.pressdemocrat.com/news/7531358-181/north-coast-fires-kindle-pot?sba=AAS.

[14] Rolling Stone, "What the California Fires Mean for the Weed Industry," 20 October 2017. [Online]. Available: https://www.rollingstone.com/culture/culture-features/what-the-california-fires-mean-for-the-weed-industry-198254/.

[15] EC - FAO Food Security Programme, "An Introduction to the Basic Concepts of Food Security," 2008. [Online]. Available: http://www.fao.org/docrep/013/al936e/al936e00.pdf.

[16] BBC News, "Fruit 'left to rot' due to labour shortages," 20 July 2018. [Online]. Available: https://www.bbc.co.uk/news/uk-scotland-tayside-central-44884882.

[17] Bloomberg, "U.K. Proposes Seasonal Worker Trial for Non-EU Farm Laborers," [Online]. Available: https://www.bloomberg.com/news/articles/2019-01-24/airbus-calls-brexit-process-a-disgrace-threatens-to-leave-u-k.

[18] SBS, "To deal with labour shortage, Australia may soon start a new visa," 18 September 2018. [Online]. Available: https://www.sbs.com.au/yourlanguage/punjabi/en/article/2018/09/13/deal-labour-shortage-australia-may-soon-start-new-visa.

[19] American Farm Bureau Federation, "Worker Shortage Threatens U.S. Ag Sustainability," 16 October 2017. [Online]. Available: https://www.fb.org/viewpoints/worker-shortage-threatens-u.s.-ag-sustainability.

[20] The Washington Post, "Google didn't lead the self-driving vehicle revolution. John Deere did.," 22 June 2015. [Online]. Available: https://www.washingtonpost.com/news/the-switch/wp/2015/06/22/google-didnt-lead-the-self-driving-vehicle-revolution-john-deere-did/?utm_term=.30419cb6e394.

[21] Link Labs, "An In-Depth Look At IoT In Agriculture & Smart Farming Solutions," 30 November 2017. [Online]. Available: https://www.link-labs.com/blog/iot-agriculture.

[22] K. G. Liakos, P. Busato, D. Moshou, S. Pearson and D. Bochtis, "Machine Learning in Agriculture: A Review," *Sensors,* 27 June 2018.

[23] National Geographic, "Why Gene Editing Is the Next Food Revolution," 10 August 2018. [Online]. Available: https://www.nationalgeographic.com/environment/future-of-food/food-technology-gene-editing/.

[24] Harvard Law School Forum on Corporate Governance and Financial Regulation, "Short Activism: The Rise in Anonymous Online Short Attacks," 27 November 2017. [Online]. Available: https://corpgov.law.harvard.edu/2017/11/27/short-activism-the-rise-in-anonymous-online-short-attacks/.

[25] UK Parliament Joint Committee on the National Security Strategy, "Cyber Security of the UK's Critical National Infrastructure," 19 November 2018. [Online]. Available: https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/1708.pdf.

[26] COPA and CGECA, CEMA, CEETTAR, ESA, Fertilizers Europe, FEFAC, ECPA, EFFAB, CEJA, "EU Code of conduct on agricultural data sharing by contractual agreement," 2018. [Online]. Available: https://copa-cogeca.eu/img/user/files/EU%20CODE/EU_Code_2018_web_version.pdf.

[27] Janzen Ag Law Blog, 15 May 2015. [Online]. Available: https://www.agweb.com/blog/janzen-ag-law-blog/what-makes-agronomic-farm-data-different-from-other-types-of-intellectual-property/.

[28] Wales Online, "£231,000 world record price paid for Deveronvale Perfection," 1 September 2009. [Online]. Available: https://www.walesonline.co.uk/news/local-news/231000-world-record-price-paid-2079744.

[29] Oxford Academic, "The role of breeding and genetics in the welfare of farm animals," Animal Frontiers: American Society of Animal Science, July 2012. [Online]. Available: https://academic.oup.com/af/article/2/3/16/4638647.

[30] USA Today, "Man arrested, suspected of killing 300,000 chickens," 8 April 2015. [Online]. Available: https://eu.usatoday.com/story/news/nation/2015/04/08/chicken-deaths-arrest/25450161/.

[31] Analytic Exchange Program, "Threats to Precision Agriculture," 2018. [Online].

[32] Iowa State University, "How far do your fruit and vegetables travel?," 2002. [Online]. Available: https://lib.dr.iastate.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1004&context=leopold_pubspapers.

[33] NCBI, "The U.S. Food and Drug Administration and Imported Food Safety," 2010. [Online]. Available: https://www.ncbi.nlm.nih.gov/books/NBK220404/.

[34] C. Osborne, "NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs," 26 January 2018. [Online]. Available: https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/.

[35] Khaleej Times, "UAE to reduce dependence on imported food products," 19 December 2017.

[Online]. Available: https://www.khaleejtimes.com/nation/uae-to-reduce-dependence-on-imported-food-products.

[36] Bloomberg Businessweek, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," 4 October 2018. [Online]. Available: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

[37] Department of Homeland Security, "Critical Infrastructure Sectors," [Online]. Available: https://www.dhs.gov/cisa/critical-infrastructure-sectors.

[38] F. Yiannas, "A New Era of Food Transparency Powered by Blockchain," 2018. [Online]. Available: https://www.mitpressjournals.org/doi/pdf/10.1162/inov_a_00266.

[39] National Institute of Standards and Technology, "NIST Special Publication 800-30 Rev. 1 Guide for Conducting Risk Assessments," September 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf.

[40] White House Press Office, "Presidential Policy Directive (PPD)," 12 February 2013. [Online]. Available: https://www.whitehouse.gov/the-press-ofce/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.