Hungarian Association of Agricultural Informatics
European Federation for Information Technology in Agriculture, Food and the Environment

Journal of Agricultural Informatics. Vol. 12, No. 2
journal.magisz.org

The importance of cybersecurity in modern agriculture

Zsanett Angyalos[1], Szilvia Botos[2], Róbert Szilágyi[3]

I N F O
Received: 26.03.2021
Accepted 12.05.2021
Available on-line: 15.06.2021
Responsible Editor: L. Varallyai

Keywords:
cybersecurity, precision agriculture, Information Technologies

A B S T R A C T

Nowadays, the use of information tools has become commonplace; we can not imagine our world without their help. As in any sector, agriculture needs to use these tools as the rapidly growing population food supplier. However, keep in mind that IT (Information Technologies) assets are threatened by severe threats and significant cybersecurity risks. Precision farming is based on IT, so the threat level is high. The are several information theories about information security, and there are researches in the field of agriculture informatics. The digitalization of agriculture is essential, but it brings new problems to many farms. Such new technologies like IoT devices (Internet of Things), blockchain seem to be useable in agricultural processes, but the possible IT breach should be handled. The agro-industry IT security is more vulnerable than ever before, but the benefits of using the technology promise to outweigh the risks.

1. Introduction

The agricultural sector plays a significant role throughout the world. The rapid development of information and communication technologies is strongly influencing the structure and procedures of modern agriculture. Today, the use of information tools has become commonplace, without their application, we cannot imagine our world. As in any sector, the use of these tools has a key role in agriculture. The problems caused by the rapidly growing population and global warming make it increasingly difficult to produce the right quantity and quality of food (Karlov, 2017). However, the spread of innovative technologies is hampered by a number of factors. In the European Union countries, primary agricultural production is still dominated by small family farms, which may not be able to afford modern systems (Jussi et al., 2020). Another major obstacle is a generational change and educational attainment, as according to Eurostat data from 2016, more than 80% of farm managers are over 45 years old and more than 50% are over 55 years old. The share of managers under the age of 40 is only 19% (Eurostat, 2016).

[1] Zsanett Angyalos Hungary
zsanett.angyalos@gmail.com
[2] Szilvia Botos
University of Debrecen,
botos.szilvia@econ.unideb.hu
[3] Róbert Szilágyi
University of Debrecen
szilagyi.robert@econ.unideb.hu

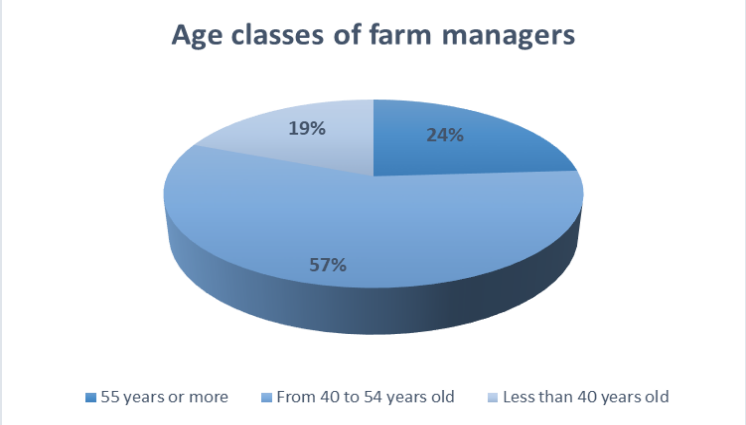

Figure 1. Age of farm managers (according to eurostat)

The aging of the farming population and the relatively low education level are major obstacles to the spread of innovative technologies. In addition, research has shown that information barriers also significantly hinder the diffusion of technologies, as farmers must first know that such a solution exists, understand how to use it, and believe that its application can improve productivity.

The Earth's population is estimated to grow to approximately 11 billion by 2100, which means we will almost have to double the amount of food produced today by then.

Therefore, it is crucial that producers, processors, and farmers use high-tech tools/systems to optimize production conditions, use resources efficiently, and reduce waste. The use of intelligent farming technologies and precision technologies can be an excellent solution. Intelligent farming technologies include data collection and processing to improve crop fields and food quality. For example, a moisture sensor placed in the ground can be used to reduce the application of excess water. Such technologies make it possible to create the right environmental conditions for plants in greenhouses or even animals (Erdeiné, 2020).

2. Information technology in precision agriculture

Precision farming is a complex concept. In this case, it is a set of tools and methods that, based on IT-technological developments, result in significantly different production technology solutions than before. They can be applied to make farming more efficient and effective while taking environmental and sustainability criteria into account (Angelita et al., 2020).

High-precision navigation and automatic machine steering are essential for precision farming. Software is also a prerequisite for precision farming, as continuous data collection and processing are required.

The continuous development of technology is bringing innovative solutions day by day. Thus, it is more and more challenging for many to follow technical developments and create the conditions for their application.

The determining element of the future of agriculture is the development of integrated systems, the interconnection of the existing ones (Figure 2).

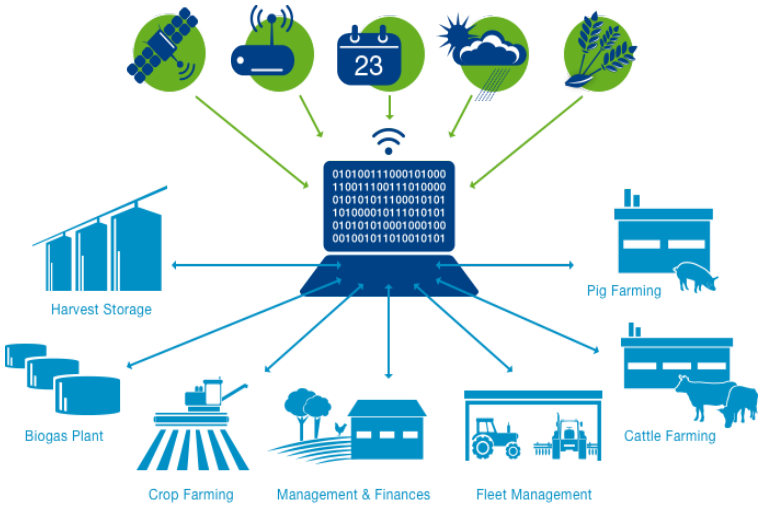

Figure 2. Interconnected Systems

However, keep in mind that IT (Information Technologies) assets are threatened by serious threats, but by significant cybersecurity risks. What about the definition of cybersecurity? „Cybersecurity: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." Department of Homeland Security: National Initiative for Cybersecurity Careers and Studies – Glossary

"The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." (DHS, 2014).

"The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this." (Oxford University Press, 2014).

2.1. Threats in precision agriculture

Systems connected to the World Wide Web can easily fall victim to "cybercriminals" who, on the one hand, can recover the data they have acquired and, on the other hand, paralyze the entire automated economy and cause any damage in this regard. Potential agricultural attacks can create an unsafe and product-less farming environment. Attackers in closed systems (smart farm, greenhouse, livestock farm) environmental conditions can be modified to destroy the plants and animals there. Furthermore, if the control systems of an automatic tractor, combine, drone are attacked, farmers will have unpredictable consequences, such as plant protection "accidents", soil poisoning, severe crop losses.

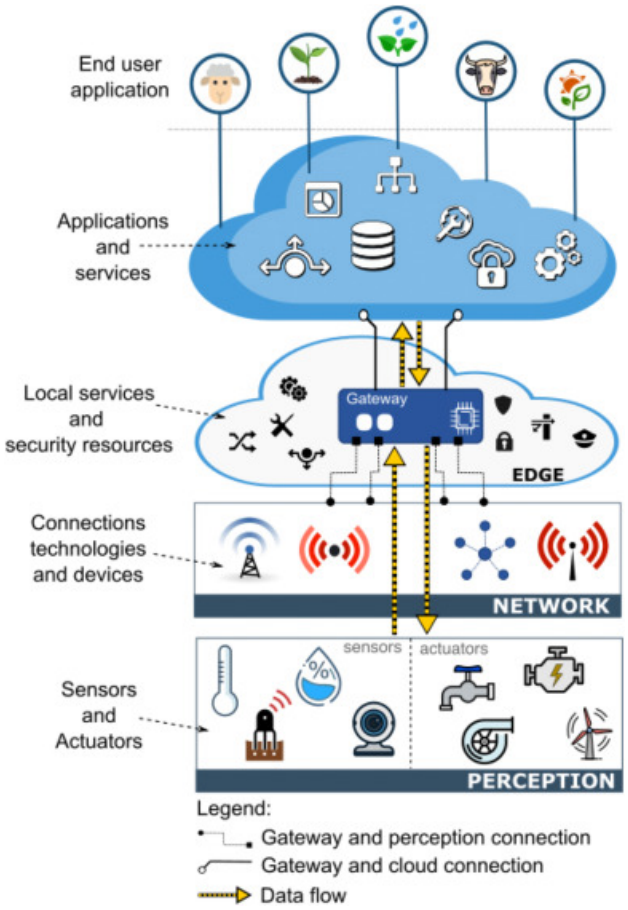

Figure 3. Connections between different systems (Angelita et al., 2020)

Figure 3 shows the interaction between endpoints between different authorizations involved in the system. Sensors and operation systems generate data, they get instructions through applications. Gateways are used to flow one piece of this data from one network to another. In the cloud, end users can access large amounts of data and information (Angelita et al., 2020). For example, from an environmental point of view, with energy-economic information, or other relevant information, the acquisition or manipulation of which could cause significant damage to the economy. Such attacks are often called agroterrorism when an agriculture-dependent economy can easily disrupt. The report, released by the U.S. Department of Homeland Security, has elaborated on various cyber threat scenarios in precision agriculture and further emphasizes the need for research on this critical topic. A sophisticated agroterrorist attack on a major exporting country has a healthier detrimental effect on millions of consumers worldwide. Also, such attacks can undermine the confidence of importing countries.

Main theories in information security

The Confidentiality, Integrity, Availability (CIA) model is a fundamental information security element (Kim and Solomon, 2012). In the CIA model, confidentiality covers data privacy; only authorized users can access the information. Integrity covers data validity and accuracy.

Availability covers the data or services being accessible. In a proper cybersecurity environment, these three aspects of information security are guaranteed. Trendov et al. (2019) mention data security regarding agricultural big data. West (2018) discusses that there are two types of precision agriculture systems - those that have been hacked and those that will be.

In general, agricultural cybersecurity is an existing problem, especially for small and medium farms, where the farms' staff are not trained to be technology experts. Therefore, the digitalization

of agriculture brings new problems to many farms that they cannot manage professionally (Nikander et al., 2020).

The consequences of the attacks

According to the World Health Organization (WHO), more than 10 million people die each year from food-related illnesses, and 600 million people get sick because food is contaminated with bacteria, viruses, chemicals. On the basis of the risks, economies do not give up the opportunities offered by IoT (Internet Of Things) systems, nor they have to give up, as they can gain a significant competitive advantage by using them. For the reasons mentioned above, farms need to be aware of such and similar threats and their prevention.

3. Transformation of agriculture

Botos et al. (2015) research focused on rural micro and small to medium enterprises about their significant economic role. With their survey, they get an answer to how firms use the internet, which are the relevant ICT for them, and what it depends on. They asked several SMEs from the North Hungarian region, 106 SMEs were interviewed. The internet usage and the ICT relevance were highly represented.

Agricultural businesses are beginning to recognize the importance of digitization. The emergence of the information economy - information as a factor of production poses new challenges (Debrenti et al., 2019).

For organizations to remain competitive in this digital era and beyond, IT must embrace digital transformation and the requisite infrastructure needed to achieve it. Today, a wide range of management support systems and tools are available for the company's efficient operation. The prerequisite for the application of these systems is the appropriate digitization of enterprises and their digital readiness (Debrenti, 2019).

Such a new technology like the blockchain seems to be useable in agricultural processes. This technology provides so many features in food tracking (Füzesi et al., 2020). Because of the data safety and the possibility of a cybersecurity attack, it could be a potential risk in the future.

The explosive growth of IoT systems and Big Data further fuel the transformation of traditional agriculture into digital, knowledge-based agriculture, where data collection, analysis, communication, and data-based decision-making are taking place at a rapid pace (Shivappa et al., 2018).

IoT devices help with data collection Sensors connected to tractors, trucks, fields, soil and plants to collect real-time data that analysts have instant access to. For example, data collected by intelligent climate monitoring systems can be used to map weather conditions and select the appropriate plant based on this. By storing the data, it allows farmers to export trends and develop appropriate growth strategies. When used in greenhouses, sensors can monitor temperature, soil moisture, humidity, and other variables, and even adjust environmental variables to ensure optimal plant growth. Furthermore, the sensors are able to measure the health, activity and nutrition of the livestock, thus providing real-time data on the health status of all animals. GPS technology makes it possible to track vehicles and animals' movements and can even give farmers a real-time view of the location of their livestock. Their movements can be tracked and traced back from previous data (Atac and Akleylek, 2019).

With such intelligent systems, vast amounts of data can be collected, analyzed, and used for more informed decision-making. With the help of Big Data, we can gain insight into various management operations and make real-time decisions. Besides, the sensors allow farmers to use automated identification tags to obtain data about the entire life cycle of a given product, thus helping to gather relevant information such as how the product is moved and stored throughout its whole life cycle (Sjaak et al., 2017).

Figure 4 shows the size of the IoT device market for 2018 and 2023. The statistician predicts that IoT devices' market value in global agriculture will reach nearly $ 30 billion by 2023.

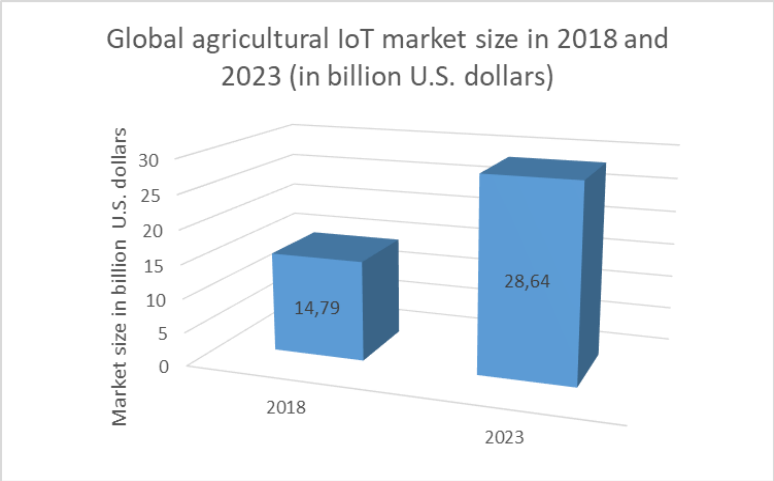

Figure 4. Global agricultural IoT market (according to Statista)

There are countries where the goal is the widespread adoption of data-based technology, while robotics and artificial intelligence have already appeared in the leading markets in agriculture. The importance of robotics is shown by the fact that the global market for robots used in agriculture is projected to reach more than $ 20 billion by 2025 (Figure 5). These innovative tools mainly help sowing, planting and irrigation, but they can also play a key role in animal husbandry, for example thanks to milking robots.

Because of this, cybercriminals pay attention to the agricultural industry, many organizations are uniquely vulnerable. After all, larger companies may have an effectively developed defense system, but smaller companies and economies have limited resources, budgets are tight, and cybersecurity is often not listed as disclosure of urgent spending.

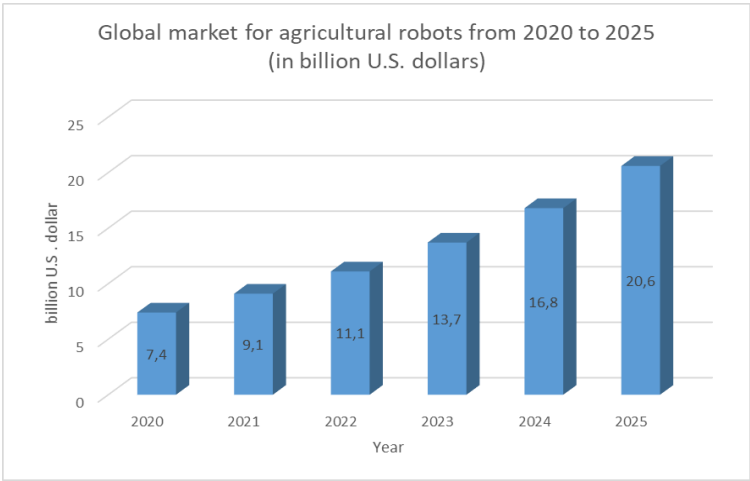

Figure 5. Global market for agricultural robots (according to Statista)

Conclusion

As the digital transformation sweeps through the agro-industry, many businesses are open to cybercriminals as the pursuit of cybersecurity far underperforms precision systems' speed. Many farmers and producers are unprepared for the threats to their systems, even they are often unaware of them. Such different threats are different in phishing emails that are designed to look real but are tricked into providing account information or downloading malware in the meantime. Malware has a wide variety of variations and is evolving. Adware tries to bombard the browser with ads, while

ransomware literally takes the computer system hostage to exclude the user from the system and release it only after paying the crisis fee.

If a farmer has to choose between a catastrophic interruption of operations and a paycheck, the paycheck is chosen, and criminals know that (Sontowski et al., 2020). Even larger companies have to struggle with recruiting people with the right expertise who provide equal and effective protection with their design. Small companies find it almost impossible to have the necessary experts, affordable people. Large economies need to protect a lot of real estates and have many opportunities to make mistakes. After all, every defense is only as strong as its weakest link.

In summary, the agro-industry is more vulnerable than ever before, but the benefits of using the technology promise to outweigh the risks. We live in a digital world where organizations that do not adopt the latest trends take the risk of lagging behind those companies that have already incorporated them into their culture. Because of this, these economies gain a significant competitive advantage.

References

Angelita R., Eduardo da S., Luiz C. P. A. (2020): Security challenges to smart agriculture: Current state, key issues, and future directions, Array, Vol. 8, 100048, ISSN 2590-0056, https://doi.org/10.1016/j.array.2020.100048

Atac C., Akleylek S. (2019). A Survey on Security Threats and Solutions in the Age of IoT.European Journal of Science and Technology, (15), 36-42.

Botos Sz., Herdon M., Várallyai L. (2015): Readiness for future internet services in rural areas. In. Procedia Economics and Finance 19. 2015. pp. 383-390. https://doi.org/10.1016/S2212-5671(15)00039-8

Debrenti A. S. (2019): Digitization landscape in the Hungarian food-processing industry, Journal of Agricultural Informatics (ISSN 2061-862X) 201X Vol. 10, No.2: 68-81 doi: 10.17700/jai.2019.10.2.544

Debrenti A. S., Csordás A., Herdon M. (2019) Management support systems in the Hungarian food manufacturing sector, Journal of Agricultural Informatics (ISSN 2061-862X) 2019 Vol. 10, No. 1:21-32 doi: 10.17700/jai.2019.1.1.498

DHS. 2014. A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. 2014.

Erdeiné Késmárki-Gally Sz. (2020) „A Precíziós Gazdálkodás Jelentősége A Mezőgazdaság Versenyképességében”, Multidiszciplináris kihívások, sokszínű válaszok - Gazdálkodás- és Szervezéstudományi folyóirat , (2), o. 43-58. doi: 10.33565/MKSV.2020.02.03.

Eurostat (2016): Farms and Farmland in the European Union – statistics. Available at https://ec.europa.eu/eurostat/statistics-explained/index.php/Farms_and_farmland_in_the_European_Union_-_statistics#Farms_in_2016 accessed at May 15th 2020.

Füzesi I., Csordás A., Reuf S., Felföldi J. (2020): Applicability of Blockchain-Based Traceability Systems in the Food Supply Chain, Journal of Agricultural Informatics (ISSN 2061-862X) 2020 Vol. 11, No. 1: 9-23 doi: 10.17700/jai.2020.11.1.562

Jussi N., Onni M., Mikko L. (2020): Requirements for cybersecurity in agricultural communication networks, Computers and Electronics in Agriculture, Volume 179, 105776, ISSN 0168-1699

Karlov A.A. (2017): Cybersecurity of internet of things - Risks and opportunities. In Proceedings of the XXVI International Symposium on Nuclear Electronics & Computing (NEC'2017), Budva, Montenegro, 25–29 pp. 182–187.

Kim, D., Solomon, M., 2012. Fundamentals of Information Systems Security. Jones & Bartlett Learning LLC.

Nikander J., Manninen O., Laajalahti M. (2020): Requirements for cybersecurity in agricultural communication networks, Computers and Electronics in Agriculture no. 179, 105776, https://doi.org/10.1016/j.compag.2020.105776

Oxford University Press. 2014. Oxford Online Dictionary. Oxford: Oxford University Press. 2014.

Shivappa H., Prakasa Rao E.V.S., Gouda K. C., Ramesh K., Rakesh V., MOHAPATRA G. N., Rao K., Sahoo S. Pp A. (2018): Digital revolution and Big Data: a new revolution in agriculture.. CAB Reviews Perspectives in Agriculture Veterinary Science Nutrition and Natural Resources. 13. 1-7.

Sjaak W., Lan G., Cor V., Marc-Jeroen B. (2017): Big Data in Smart Farming – A review, Agricultural Systems, vol 153, pp. 69-80, ISSN 0308-521X, (https://doi.org/10.1016/j.agsy.2017.01.023.)

Sontowski S., Gupta M., Chukkapalli S.S.L., Abdelsalam M., Mittal S., Joshi A., Sandhu R. (2020). Cyber attacks on smart farming infrastructure. UMBC Student Collection.

Trendov, N.M., Varas, S., Zeng, M., (2019): Digital technologies in agriculture and rural areas. Briefing paper. Food and Agriculture Organization of the United Nations, Rome.

West, J., 2018. A prediction model framework for cyber-attacks to precision agriculture technologies. J. Agric. Food Inf., 19(4), pp. 307–330 (https://doi.org/10.1080/10496505.2017.1417859)