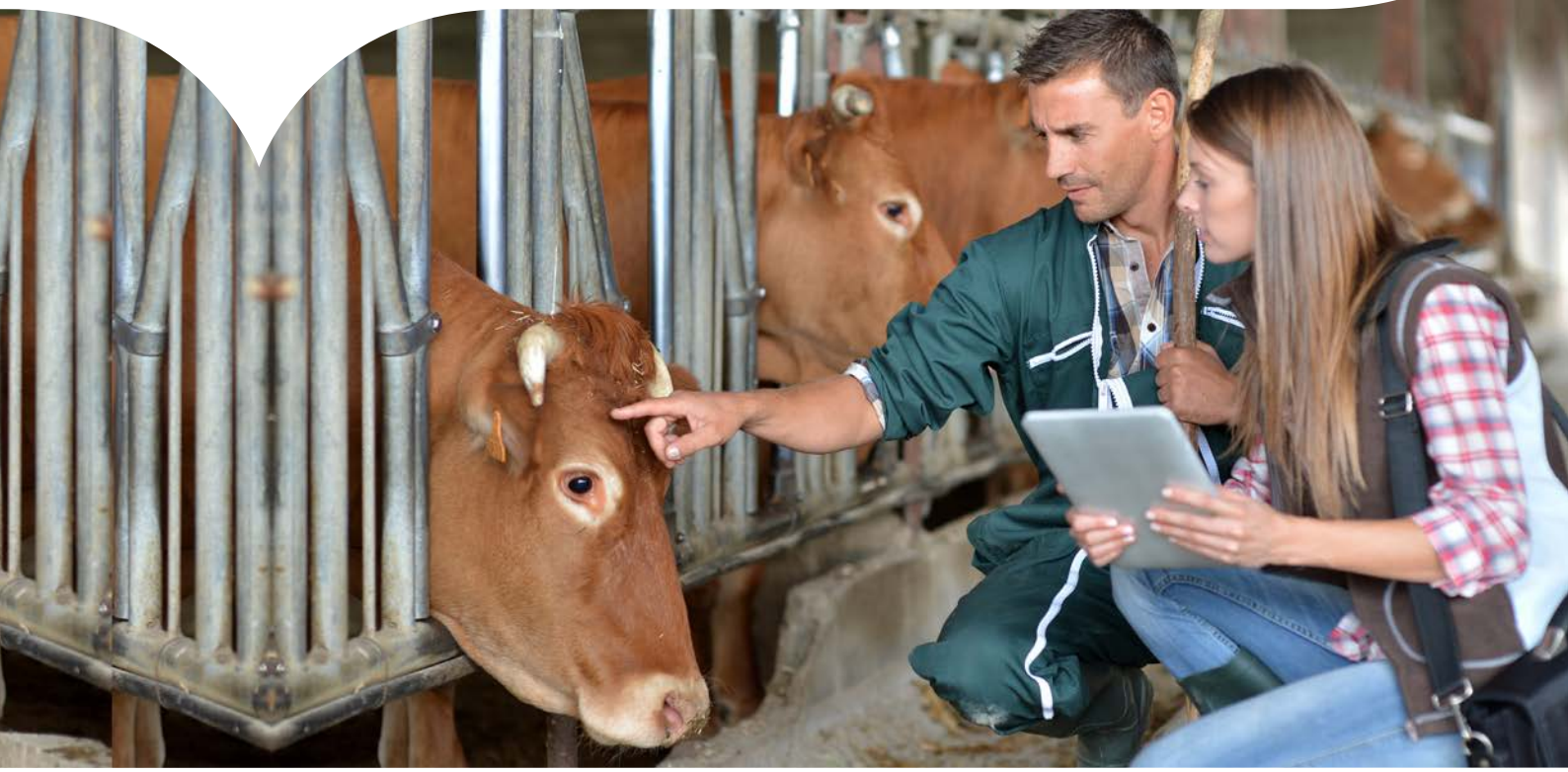
Capgemini Consulting

WAGENINGEN UR
For quality of life



Cybersecurity in the Agrifood sector

Securing data as crucial asset for agriculture

Protect your data just like your resources

Every day new digital applications find their way into our lives. Digitization has brought our society many benefits and will do so for the coming years as key enabler for our economy. It is an important driver behind innovation and economic growth. This development speeds the hyper connected world, in which everyone and everything can and probably will be connected by and through the Internet. Progresses in connectivity possibilities have made access to information much easier and cheaper. New innovative business models (in mobility, banking or e-health) are replacing the older business models. However, to create sustainable innovation and frequent use, security is absolutely essential. Due to the increased frequency of high tech possibilities, the chance of technical failure or severe misusage and abuse of vulnerabilities can become a realistic threat. Several sectors have devised focused strategies on cybersecurity. For example, banking and insurance see client threat management as an increasing priority[1]. To put the urgency in words “The more we depend on data, the more we depend on its security”.

The more we depend on data, the more we depend on its security

The agrifood sector has many data-driven innovations. Paper trail Information streams in this sector that previously existed are already more digitized due to long-term innovation[1]. The sector is more and more dependent on availability, reliability and confidentiality of business data. When data needs to be continuously available, its vulnerability is a threat for the primary process.

[1] Poppe, K, S. Wolfert, C. Verdouw and T. Verwaart (2013). Information and Communication Technology as a Driver for Change in Agri-food Chains in: EuroChoices vol 12. Nr. 1, 1 2013 pages 60–65.

> *Data in the agrifood sector becomes more and more important. It is becoming an important asset not only for the business process but also for the entire food supply chain.*

Through the introduction of advanced sensing and monitoring technology the agri-food sector increasingly uses the possibilities of the "Internet of Things" as well as access to data from third parties. Process automation in milking and crop production, site-specific application of fertilizers and crop protection based on combinations of sensors and other data sources in the chain (including market information and phenotypical data) delivers large amounts of data[2].

Take the tremendous growth of automatic milking systems, with approximately 10,000 farms across the globe milking more than 1.2 million cows unmanned. Northern Europe, the Netherlands, Germany and France are leading the shift towards automatic milking. 90% of new equipment installations in Sweden and Finland, and 50% in Germany include robotic milking[3]. According to Lely, an international manufacturer of agricultural machines, almost half of the dairy herds in north-western Europe will be milked by robots in 2025[4]. The Netherlands is the country with the largest number of automatic milking farms in north-western Europe[5]. In September 2015, more than 3,600 farms in the Netherlands have an automatic milking system[6]. Robotic milking is not only milking of milk, but also of data. It generates almost 120 variables per cow per day. The data can be divided into five categories: systems management (e.g. milkings per cow per day and box time), milk production variables (e.g. milk yield, fat, protein and lactose), udder health and milk quality (e.g. milk color, milk temperature and somatic cell count), nutrition and general cow health (e.g. how much pellet was fed, bodyweight, rumination and milk enzymes), and reproduction (cow activity and milk progesterone levels)[7].

Wireless sensor networks are quickly becoming more frequent by the agricultural industry. The majority of wireless sensor networks have been developed for research purposes. RFID is a booming trend with adoption by producers, food processing and handling industry, and merchants to establish "traceability system"[8].

The global market size for agricultural robots was $817 million in 2013 and is expected to reach $16.3 billion by 2020. The primary applications of agricultural robots are weed control, site-specifying spraying, automated harvesting and picking. Also related to the growth of agricultural robots are autonomous navigation in the fields, automated operations like seeding, unmanned automated vehicles, cooperative robots, autonomous plowing, adaptive robots, and computer vision[9].

The use of Global Navigation Satellite Systems (GNSS), of which GPS is the most commonly used in piloting tractors and to track the position of livestock, is growing The use of GNSS in livestock management has been suggested in animal monitoring (oestrus and illness detection), movement and pasture use (grazing patterns), herd location (free range cattle) and virtual fencing[10]. It is estimated that GNSS penetration into EU tractors will rise from around 7.5% in 2010 to 35% in 2020 with sales rising from c. 100,000 units p.a. in 2010 to more than 500,000 in 2020 with tractor guidance and variable rate technology being the main applications[11].

---

[2] Lokhorst, K., K. Poppe, B. Vermeer (2015). Advice on Big Data. Wageningen UR.

[3] Rodriguez, F. (2012). The realities of robotic milking technology today. In: Progressive Dairyman.

[4] Beekman, J. and R. Bodde (2015). Milking automation is gaining popularity. In: Dairy Global. http://www.dairyglobal.net/Articles/General/2015/1/Milking-automation-is-gaining-popularity-1568767W/. Website consulted in October 2015.

[5] Bisaglia, C., Z. Belle, G. van den Berg, J.C.A.M. Pompe (2012). Automatic vs. conventional feeding systems in robotic milking dairy farms: a survey in the Netherlands. CIGR-AgEng 2012 International Conference of Agricultural Engineering.

[6] KOM (2015). Statistiek. Overzicht soorten/typen melkstallen. Stichting Kwaliteitszorg Onderhoud Melkinstallaties. Dronten. http://www.stichtingkom.nl/index.php/stichting_kom/category/statistiek. Website consulted in October 2015.

[7] Lee, K. (2015). Management decisions enhanced with robotic milking data. March 31th 2015. See: http://www.progressivedairy.com/topics/management/management-decisions-enhanced-with-robotic-milking-data (consulted 16th November 2015).

[8] Caldwell, D.G. ed. (2012). Robotics and automation in the food industry. Current and future technologies. Woodhead Publishing.

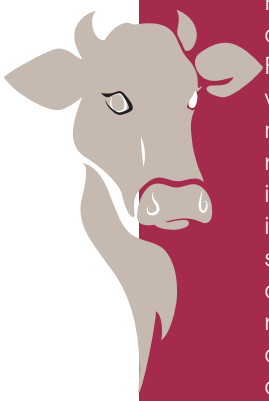
Data about products, how they are produced, processed and preserved through the entire food supply chain, via automatic ID technology, produces an important data source for tracking & tracing and early warning systems. Via smartphones, wearables and sensors, an enormous amount of data about livestock is collected. Analysis of these data can lead to better insights for tailor made advice to farmers. That ensures further optimization and sustainability of business in the agrifood sector and prevents resources waste[12].

We estimated that around 50 percent of all the large and medium-sized arable farmers (with 20 acres and more) in the Netherlands have a business management system (BMS). Initially growers use their BMS for recording production data concerning food safety requirements and provide it to their customers. The BMS is used to a limited extent for analyzing or improving internal business operations, or data exchange with external devices of their cooperatives such as CZAV, Agrifirm, Suiker Unie and Nedato[13].

“The exchange and linking of data in the agri-food sector is increasing.”

In the USA Farmers Business Network (FBN), a farmer-to-farmer data platform already has agronomic data from nearly 7 million acres of farmland across 17 states. Farmers have submitted their data, and the FBN benchmarks it against other farms nationwide, finding the best seeds for the soil of the farmers, providing farmers with a review of hundreds of agricultural products[14]. Furthermore around 150 corn farmers with 40,000 planted acres in four states of the USA have been testing FieldScripts, a software package for farmers based on farmers’ data on two years of yield data, to optimize the yield potential with variable rate seeding. The software has also been tested for soybeans and will be available in 2016, followed by software for multi-hybrids[15].

Case “Data exchange in Dairy Farming in the Netherlands”[16]



In 2013, the Smart Dairy Farming pilot project started as an initiative of the companies CRV, AgriFirm and FrieslandCampina in the Netherlands. The aim of the project is to extend the life of a cow with two years and consequently, the cow will serve five lactations instead of three. That will result in 20,000 kilogram more milk. For a dairy farm with 100 cows that means an increase in profit of around 40,000 euro. Besides CRV, a wide variety of companier such as: Agrifirm, FrieslandCampina, seven dairy farmers, the robotic milking system manufacturer Lely, software providers Rovecom and S&S Systems, accountancy AcconAVM, education and research institutes, universities, fencing manufacture Gallagher, and sensor manufacture Sentron participate in the project. The focus of this project is on the breeding of young cows, the period around calving and fertility. At the dairy farms a large amount of data about the behaviour of the cows is being collected with existing sensor technologies (like a robotic milking system and dairy cow pedometers) and new technologies. The collected data concerns the water intake, milk intake, feed intake, cow weight development, metabolism, ruminating behaviour, activity, place in the cow shed, body temperature, milk yield, and milk composition (its colour, temperature, lactose, fat content and protein content). Afterwards, the data is linked to other data from other parties in the chain such as the composition and nutritional value of the food and the milk composition. All the data will be put together and stored in an online database. Subsequently, the data will be analysed and translated into recommendations and protocols for the dairy farmers. The online database is supervised by a foundation, established by the three founding companies.

[9] Eustis, S. (2014). Agricultural Robots Market Shares, Strategy, and Forecasts, Worldwide, 2014 to 2020. WinterGreen Research Inc., Massachusetts. USA.
[10] Spink, A. et al. (2013). Animal behaviour analysis with GPS and 3D accelerometers, conference paper.
[11] GSA (2012). GNSS Market Report. Issue 2.
[12] Lokhorst, K., K. Poppe, B. Vermeer (2015). Advice on Big Data. Wageningen UR.
[13] Janssens, S.R.M. et al, (2013). Bedrijfsmanagementsystemen in de akkerbouw. Een inventarisatie van gebruik en wensen. Den Haag. LEI.
[14] Lapowsky, I., (2015). How farmers can use data push back against big ag. In: Wired. http://www.wired.com/2015/05/farmers-business-network/ Website consulted in September 2015.
[15] FieldScripts (2015). http://www.fieldscripts.com/Pages/default.aspx. Website consulted in September 2015.
[16] http://www.smartdairyfarming.nl/ Website consulted in October 2015.

“Vulnerabilities in software are still the weak spot in digital security.”

Upcoming cyber threats to agrifood businesses

As illustrated above, the agrifood sector has transformed itself into a more data-driven and complex ecosystem[17]. Companies have become increasingly dependent on IT in their primary processes and almost 100% availability is required these days. Growing digital requirements and trends (for example mobility, cloud computing, IoT, big data) continue to pose new challenges when it comes to cybersecurity. Technology like data platforms, wireless sensor networks, RFID, GPS, business management systems can be vulnerable to breakdown, abuse and misuse. What are the actual threats to agrifood businesses?

Software is a crucial part of the digital infrastructure in the agrifood sector. Vulnerabilities in software and systems remain relentlessly high. According to CSAN 2015[18] software suppliers in 2014 released thousands of updates in order to repair vulnerabilities in their software. This is the main problem when it comes to cybersecurity. The lack of IT sustainability becomes more and more a problem because a lot of software cannot easily be updated, especially in process control systems[19]. As long as the “updates” have not been installed, parts of their network will continue to be vulnerable. This problem has still not been resolved adequately and allows actors to abuse these vulnerabilities.

Let’s not forget that human error, technical or system failure and natural causes are still a major cause for ICT incidents and failure. Most of the time these system failures are software bugs, hardware failures and software misconfigurations[20]. But outage can also have an external cause. For example, power failure is among the most common causes for IT failure[21].

Vulnerabilities are only weak spots when they are abused. According to multiple government reports, professional criminals and state actors have become a serious risk for business and governments[22]. Criminals become more professional and have more equipment and tooling to execute cyber hacks. Data, money and other valuable assets such as intellectual property, confidential business data, personal information and the continuity and integrity of digital processes can be abused by malicious actors.

A secure chain is only as strong as the weakest link

Challenges are not only visible on an organizational level, but are strongly chain focused. The agrifood sector is operating in chains or networks and is dependable on other chain organizations or third parties. Some risks are obscured and/or displaced outside an organization’s span of control. A secure organization, chain and network are therefore a shared responsibility. When managing the risks of the whole chain, it is important to identify not only the physical chain, but also the “digital chain”. This chain effect has been proven in other sectors by, for example, the disruptions that occurred some time ago by DDoS attacks on Dutch banks, government departments such as DigiD[23] and - when it comes to system failures - the power failures in Noord-Holland[24]. The impact of a non-functioning chain is exceptionally high and costly[25]. A secure chain is only as strong as the weakest link.

---

[17] Poppe, Krijn, Sjaak Wolfert, Cor Verdouw and Alan Renwick (2015): A European perspective on the economics of big data in: Farm Policy Journal, Vol. 12, no. 1, autumn quarter 2015 p. 11-19

[18] Ministry of Security and Justice. National Cyber Security Centre (2015) Cyber Security Assessment. The Hague

[19] http://www.kaspersky.com/enterprise-security/industrial. Website consulted in October 2015.

[20] Enisa (2015). Annual Incidents report 2014. Incident reports about severe outages across the EU.

[21] For example the power cut in Noord-Holland/Flevoland March 2015: http://www.dutchnews.nl/news/archives/2015/03/train-chaos-after-massive-power-failure-in-noord-holland/

[22] Ministry of Security and Justice. National Cyber Security Centre (2015) Cyber Security Assessment. The Hague

[23] Ministry of Security and Justice. National Cyber Security Centre (2014) Cyber Security Assessment - The Hague Quote European Commission

[24] http://www.dutchnews.nl/news/archives/2015/03/train-chaos-after-massive-power-failure-in-noord-holland/

[25] CA Technologies (2011). Avoidable Cost of Downtime 2010. The impact of IT downtime on employee productivity.

> *Organizations often wait to take the required actions until IT systems are already experiencing continuity problems.*

A successful cybersecurity attack can have major impact, not only on the IT side but especially on the business. Some consequences are loss of reputation or loss of business due to system downtime (for example costs of not-harvesting). For an organization to take control, it has to ask itself: Are our digital "crown jewels" and reputation adequately protected and under control? And if my system fails, is my business resilient enough to recover?

Total security is an illusion and in most cases impossible to achieve, due to the substantial impact security measures can have on society and individuals. To find the balance in security, freedom, social and economic growth has become a challenge nowadays. We can combine digital innovation and transformation within acceptable risks. To cope with these vulnerabilities and threats, multiple technical solutions or standards can help to mitigate threats and risks. But improving cooperation - both internal and external at various levels - by sharing knowledge, expertise and experiences is one of the basics in developing cybersecurity resilience in the organization and the agrifood chain.

Agrifood processes not considered "vital" by government

In 2010 the Dutch government labeled several sectors as being "vital". In 2015 this process was repeated but now from the perspective of vital processes instead of vital sectors. This time agrifood processes were not labeled as vital. They were assessed as being too fragmented and therefore incapable of disrupting society or the economy. But how much impact does it have when processes for assuring food quality and food production seem vulnerable to cyber threats? Is this assessment changing with the fast digitalization of the food chain? When a shortage in crops or unreliable quality manifests, societal unrest arises. But when vulnerabilities and outages of continuity become reality, the food production processes and geographic distribution of the products will show to have a great level of resilience due to the vast networks of the food supply chain. No branch of the food chain will be threatened as a result of outages in the major food production locations. Moreover, when food supply is thin, products can be replaced by similar or alternative products to balance the shortage. This is why food production and distribution processes are not categorized as "vital infrastructure" by the Dutch government (2015).

But the vulnerabilities of the (digital) food supply chain is more and more dependable on other products and services that are labeled as "vital", of which the most important ones are drinking water, energy en transport. Besides continuity and security of food supply, food safety and quality control are vital pillars of the food business. But what happens when fraud is committed? Our attention has been drawn to the fact that there is no information on how little attention there is for cybersecurity as a consolidating factor in data on quality of produced food in an ever digitalizing chain[26].

Agrifood businesses struggle with cyber security measures

Agrifood companiess support[27] the view that digital data exchange is increasing in the agrifood sector. They mention not only technology as a main driver, but also the growing need for traceability, increasing need of customers and consumers for information on sustainability and further globalization of our food supply chains. Indeed, data is considered as a valuable asset for companies in the agrifood sector. Farm data is seen as farmers' new product alongside its crops and animals, and needs appropriate security.

[26] Protection vital infrastructure 2010 & reassessment critical infrastructure 2015 (voortgangsbrief nationale veiligheid).

[27] For this point of view several businesses active in the agrifood chain were interviewed by us on trends and their opinions on cyber security threads and the impact thesemight have on business continuity.

According to the companies interviewed, sensitive data in the agrifood sector particularly concerns business data, being valuable information for the market and its competitors. For instance food product prescriptions but also plans for take-over are considered as market-sensitive data. And for each food supply chain (dairy, meat, vegetables etc.) in the agrifood sector the risks and vulnerabilities will be different. Cyber attacks by hacktivists in order to damage the reputation of companies are seen as an increased threat. Also the increase of extortion was named in which firm data is taking hostage.

Some businesses wonder whether the agrifood sector has sufficient awareness of cybersecurity compared to other sectors. It seems that awareness in the IT and software companies as service provider of the agrifood sector, is high enough. And large food enterprises (especially multinationals) also seem to be reasonably aware of cybersecurity. Also due to their accountancy firms that carry out risk assessments and impose arrangements to meet cybercrime attacks. And also because of the new stricter privacy and data protection regulation with the obligation for data controllers to notify data breaches and higher fines.

So how should the agrifood sector deal with cybersecurity taking into account that a lot of agrifood chains operate in an international environment, crossing borders, and dealing with different legislation? Also the different cultural biases and legal systems between US, Europe and Asia on cybercrime should be taken into account. Opinions vary on how a joint approach should look like. Who should take responsibility, who will organize it and who should be involved? The large and more powerful companies in the agrifood sector such as multinationals or European purchasing alliances of the supermarket groups? And how will the costs and benefits be divided among the involved parties along the food supply chain?

- How vital is data security for your primary processes?
- How to assess risks in your digital chain?
- How to organize cyber security in your company, supply- and digital chain?
- How to create optimal governance structures for organizing cyber security with a role for governments and businesses?

Capgemini Consulting with its digital and organisational expertise combines forces with the scientific and sector expertise of Wageningen UR. For more information contact:

Capgemini Consulting

Dinand Tinholt
Vice President
Global EU lead
Tel: +31 6 2715 9294
Email: dinand.tinholt@capgemini.com

Evelien van Zuidam MSc
Senior Consultant
Security & Privacy
Tel: +31 30 689 3114
Email: evelien.van.zuidam@capgemini.com

LEI Wageningen UR

Drs Krijn Poppe
Research Coordinator
Tel: +31 70 33 58 313
Email: krijn.poppe@wur.nl

Marc-Jeroen Bogaardt BSc MA
Senior Researcher
Tel: +31 70 33 58 257
Email: marc-jeroen.bogaardt@wur.nl

Capgemini Consulting

About Capgemini Consulting

Capgemini Consulting is the global strategy and transformation consulting organization of the Capgemini Group, specializing in advising and supporting enterprises in significant transformation, from innovative strategy to execution and with an unstinting focus on results. With the new digital economy creating significant disruptions and opportunities, the global team of over 3,000 talented individuals work with leading companies and governments to master Digital Transformation, drawing on their understanding of the digital economy and leadership in business transformation and organizational change.

Find out more at:

www.capgemini-consulting.nl

The mission of Wageningen UR (University & Research centre) is 'To explore the potential of nature to improve the quality of life'. Within Wageningen UR, nine specialised research institutes of the DLO Foundation have joined forces with Wageningen University to help answer the most important questions in the domain of healthy food and living environment. With approximately 30 locations, 6,000 members of staff and 9,000 students, Wageningen UR is one of the leading organisations in its domain worldwide. The integral approach to problems and the cooperation between the various disciplines are at the heart of the unique Wageningen Approach.

Find out more at:

www.wageningenur.nl

Capgemini Consulting
P.O. Box 2575, 3500 GN Utrecht
Tel. + 31 30 689 00 00
www.nl.capgemini-consulting.com

IN/02-029.16 © shutterstock.com