Virginia Cooperative Extension
Virginia Tech • Virginia State University
www.ext.vt.edu

The Emergence of Cyberbiosecurity Concerns in Food and Agriculture

Authored by Rebekah J. Miller, Graduate Research Assistant, Department of Food Science and Technology, Virginia Tech; Susan E. Duncan, Associate Director, Virginia Agricultural Experiment Station, Virginia Tech; and Laura K. Strawn, Associate Professor and Extension Specialist, Food Science and Technology, Virginia Tech

What is cyberbiosecurity?

Cyberbiosecurity is an emerging discipline at the interface of cybersecurity, cyber-physical security, and biosecurity (Figure 1) (Duncan et al., 2019; Murch et al., 2018). Cyberbiosecurity differs from other disciplines as it focuses on the protection of biological data and information related to biological data that is stored, shared, or accessed using technology or a virtual platform.

As the food and agricultural industry incorporate processing automation, virtual data and information storage, and new technologies, security of these systems and processes are left at risk of cyberattacks (Figure 2).

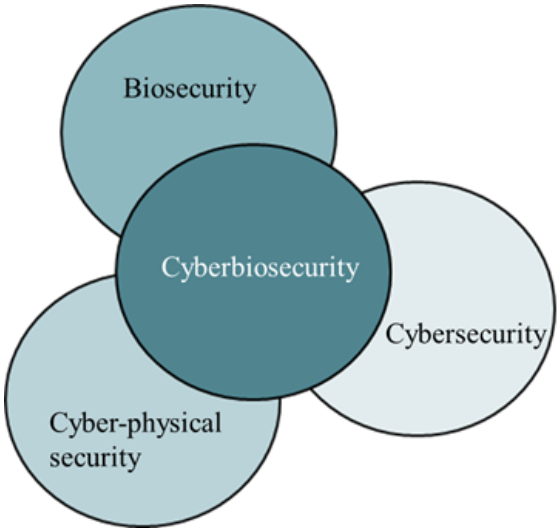

Figure 1. Cyberbiosecurity is an emerging field between biosecurity, cybersecurity, and cyber-physical security (Murch et al., 2018) (Figure adapted from a figure by Duncan et al. (2019))

Figure 2. Technology and advanced equipment used in the food and agricultural industries contribute to efficiency but can bring risk of cyber-attack (Photo by Loren King on Unsplash).

Automation and technology causing vulnerabilities can include:

- GPS equipment or trackers
- Automatic sensors
- Processing automation
- Industry or business software
- Management systems
- Cyber storage of data or records
- Use of cellphones and laptops
- Electronic building security

Much of the technology integrated into the food and agricultural industry supports or conducts collection or data or storage of data and information. This data is often used for decision making meaning the security and integrity of the data a vital piece to the safety of the system and a major concern for food and agriculture within cyberbiosecurity (Duncan et al., 2020).

Who should be concerned about cyberbiosecurity?

Cyberbiosecurity is important for everyone contributing to the food supply chain from farm to fork. Vulnerabilities to cyber threats can exist throughout the entire supply chain (Murch et al., 2018) which can result in weakness of the entire supply chain as security is only as good as the weakest point in the system (Drape et al., 2021). All levels of employees including field and plant workers, supervisors and managers, laboratory staff, auditors, and truck drivers need to be understanding of the cyberbiosecurity risks and warning signs. Due to the level of technological integration, cyberbiosecurity cannot fall to the IT department or resources for the food and agricultural industry. Cyberbiosecurity is bigger than one employee or department. Successful cyberbiosecurity will include all employees and contributors.

Past, current, and future integration of technologies and reliance on cyberspace for communications and data storage throughout the food and agricultural industries will continue to create and expose vulnerabilities and security gaps. Integration of cyberbiosecurity strategies in food and agriculture will bring a heightened security of the food supply (S. E. Duncan et al., 2019).

What are the main concerns?

The main concerns related to cyberbiosecurity can be broken into four large categories (Figure 3) (Schmale et al., 2019):

1. Data Injection
2. Automated System Hijacking
3. Node Forgery
4. Learning Algorithms Risk

Data injection refers to addition of faulty data into a system or dataset (Schmale et al., 2019). Data sets are used throughout the food and agricultural industry to check process controls and dictate decisions. Tampering with this data could result in continuous operation of systems and processes outside of their acceptable control limits or decision outcomes which cause harm to consumers or the system.

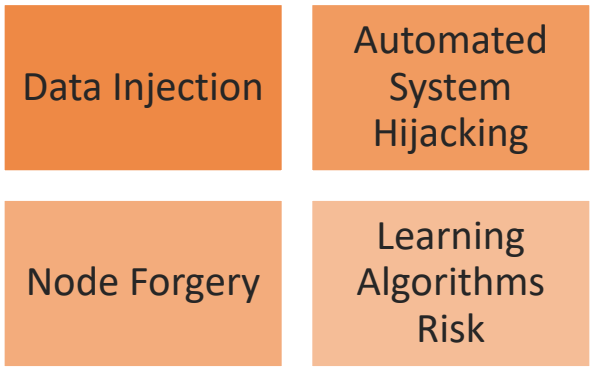

Figure 3. Cyberbiosecurity concerns can be organized into four main categories, (1) data injection, (2) automated system hijacking, (3) node forgery, and (4) learning algorithms risk (Schmale et al., 2019).

Automated system hijacking refers to loss of control over an automated system due to a cyberattack (Schmale et al., 2019). As food and agricultural processes become more automated, an automated system hijacking event could be extremely disruptive for the food supply. Loss of control over one system will halt the connected portions of the supply chain and can cause an increase in food waste, reduction in efficiency, reduced product supply, and increased product demand and price. The economic strain caused by such an event would be higher for small scale farmers and producers in the supply chain.

Node forgery refers to a false identity of sensors including sensors used to increase growing efficiency or optimize a food processing operation (Schmale et al., 2019). As growers continue to implement use of sensors for data collection around weather conditions such as temperature and humidity or soil health and conditions such as temperature, moisture, and pH, the total number of sensors in use throughout the food supply will increase concerns around sensor identity, safety, and security.

Learning algorithms risk includes vulnerability of machine learning systems which could result in threats to data (Schmale et al., 2019). Systems and processes building their capabilities and incorporating learning algorithms could be negatively impacted by cyber-attacks in this area.

Why should you be concerned?

Cyber-attacks in food and agriculture can negatively impact food safety and quality, production abilities, transportation, product supply, and the entire supply chain. Understanding the risks associated with cyberbiosecurity and building knowledge around vulnerabilities and mitigation strategies through the food and agricultural industry will build a safer, more reliable supply chain.

Schreiber Foods, a Wisconsin company who produces a variety of dairy products, fell victim to a cyberattack in the fall of 2021 (Shepel and Bollier, 2021). The attack stopped operations at all facilities and required a full five days to recover causing chaos for the milk supply chain as deliveries in transit had to be rerouted and production schedules adjusted (Shepel and Bollier, 2021). Though the facilities were fully operable a week later, this cyber-attack was ultimately to blame for a cream cheese shortage felt by consumers nationwide weeks after operations had been restored (Maruf, 2021). The timing of this shortage came around the winter holidays causing frustration for consumers hoping to make dishes and desserts requiring cream cheese (Maruf, 2021).

Best Practices

Implementing some best practices where possible may help reduce the likely hood of a cyber-attack occurring. These practices may include (Figure 4) (Carneiro et al., 2021):

- Train employees on cyber risks and safety practices
- Limit access to computers, phones, and other devices through physical barriers and passwords
- Always use strong passwords or passphrases that are unique to the user and known only by the user
- Implement a multi-factor authentication process for logging into systems or databases
- Keep software, applications, and devices update to date

Figure 4. Keeping software, applications, and devices such as laptops and cellphones up to date is an important piece of cyberbiosecurity practices (Photo by Clint Patterson on Unsplash)(Carneiro et al., 2021).

Contributing Practices

Some food safety and food defense strategies positively contribute to cyberbiosecurity. Good record keeping, traceability, chemical management, and a variety of other prerequisite programs contribute to strong food safety and food defense culture but can also contribute to a strong cyberbiosecurity culture. Employees following best practices and speaking out when they see something abnormal or below standard can help catch a cyber-attack providing a chance to mitigate the issue. Food scientists and food industry employees are understanding of preventive and corrective measures as well as the importance of mitigating threats of all types (Duncan et al. 2021). Building an awareness of the cyber threats in addition to the physical, chemical, and biological threats is a small start to building a stronger, safer food supply chain.

Warning Signs

The delicate nature of our food supply chain adds urgency to the need for awareness of cyberbiosecurity. Even with preparation, a cyber-attack may be unavailable in some cases. Additionally, they can be challenging to identify. Some cyber-attacks will cause issues with access and use of usual files, programs, or devices and while they may at first seem like an odd fluke, these issues could be a sign of cyber-attack. Examples of probable red-flags can include (Ministry of Health, 2021):

- Unable to access common files or applications
- Password changes without users' knowledge
- Software having been installed or uninstalled without users' knowledge
- Files being encrypted without users' knowledge
- Slower internet speeds
- Suspicious or abnormal pop-ups when using the internet
- Email activity without the user's knowledge
- Unable to control the computer

Identifying a red flag is the first necessary step to recover from a cyber-attack. Next steps should include disconnecting the device from the internet then unplugging the internet router (ESDS, 2022). Involving a specialist would be advised to ensure you can quickly shut down the issue and avoid further risk before starting the recovery process.

References

Carneiro, Renata, Susan Duncan, Ford Ramsey, Hasan Seyyedhasani, and Randall Murch. 2021. "Cyber attacks in agriculture: protecting your farm and small business with cyberbiosecurity." Virginia Cooperative Extension. https://caia.cals.vt.edu/content/dam/caia_cals_vt_edu/cyberbiosecurity/2021%20Carneiro%20et%20al%20Cyberattacksinagricultureprotectingyourfarmandsmallbusinesswithcyberbiosecurity.pdf

Drape, T., Magerkorth, N., Sen, A., Simpson, J., Seibel, M., Murch, R. S., & Duncan, S. E. (2021). "Assessing the Role of Cyberbiosecurity in Agriculture: A Case Study." *Frontiers*; WorldCat.org. https://doi.org/10.3389/fbioe.2021.737927

Duncan, Susan E., Robert Reinhard, Robert C. Williams, Ford Ramsey, Wade E. Thomason, Kiho Lee, Nancy Dudek, Saied Mostaghimi, Edward Colbert, and Randall S. Murch. 2019. "Cyberbiosecurity: A New Perspective on Protecting US Food and Agricultural System." WorldCat.org. https://doi.org/10.3389/fbioe.2019.00063.

Duncan, Susan E., Bo Zhang, Wade Thomason, Margaret Ellis, Na Meng, Michael Stamper, Renata Carneiro, and Tiffany Drape. 2020. "Securing Data in Life Sciences—A Plant Food (Edamame) Systems Case Study." *Frontiers in Sustainability* 1. https://www.frontiersin.org/article/10.3389/frsus.2020.600394.

Duncan, Susan, Renata Carneiro, Jonathan Bradley, Melissa Hersh, Ford Ramsey, and Randall Murch. 2021. "Beyond Ransomware: Securing the Digital Food Chain." *Food Technology Magazine*. https://www.ift.org/news-and-publications/~/link.aspx?_id=A0625C29CA904AFB8FA31CDF794CA3A9&_z=z

Maruf, Ramishah. 2021. "The Surprising Reason You Can't Find Cream Cheese Anywhere." *CNN Business*. https://www.cnn.com/2021/12/18/business/cream-cheese-cyberattack-schreiber-foods/index.html

Murch, Randall S., William K. So, Wallace G. Buchholz, Sanjay Raman, and Jean Peccoud. 2018. "Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy." *Frontiers in Bioengineering and Biotechnology* 6. https://www.frontiersin.org/article/10.3389/fbioe.2018.00039.

Schmale, David G., Andrew P. Ault, Walid Saad, Durelle T. Scott, and Judy A. Westrick. 2019. "Perspectives on Harmful Algal Blooms (HABs) and the Cyberbiosecurity of Freshwater Systems." *Frontiers in Bioengineering and Biotechnology* 7. https://doi.org/10.3389/fbioe.2019.00128.

Shepel, Jan, and Jeff Bollier. 2021. "Green Bay-based Schreiber Foods Resuming Production after Cyber Event." *National Cyber Security News Today*. https://nationalcybersecuritynews.today/green-bay-based-schreiber-foods-resuming-production-after-cyber-event-emailsecurity-phishing-ransomware/

Additional Sources

ESDS. 2022. "Signs of Cyber Attack and How to Respond to them?" https://www.esds.co.in/blog/signs-of-cyber-attack-and-how-to-respond-to-them/#:~:text=Red%20Flags%20of%20a%20Potential%20Cyber%20Attack&text=Unknown%20software%20appears%20or%20suddenly,turn%20off%20without%20your%20involvement.

Ministry of Health, Singapore. 2021. “Common Signs of a Cyber-Attack.” https://www.moh.gov.sg/licensing-and-regulation/cybersecurity-for-healthcare-providers/common-signs-of-a-cyber-attack.

Visit Virginia Cooperative Extension: ext.vt.edu

2022 FST-440NP