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

Cyberbiosecurity for Small Fermentation Businesses: Recommendations for Integration with Known Hazard Prevention Tools

Authored by Jordan Reisterer Knapp, Graduate Student, College of Agriculture and Life Sciences, Virginia Tech; Alexis M. Hamilton, Assistant Professor and Extension Specialist, Department of Food Science and Technology, Virginia Tech; Brian Wiersema, Pilot Plant Manager, Department of Food Science and Technology, Virginia Tech; Joe Eifert, Professor and Graduate Program Director, Department of Food Science and Technology, Virginia Tech; Laura K. Strawn, Associate Professor and Extension Specialist, Department of Food Science and Technology, Virginia Tech

Cyber-attacks and Small Businesses

Small businesses have a higher chance of cyber-based attacks, due to the use of home internet-linked computers for personal and business needs (Duncan et al., 2019). Twenty percent of small businesses have been hacked (Duncan et al., 2019), showing that cyber-attacks are not limited to larger businesses and corporations. The growing pressure of small businesses to adopt a digital presence (e.g., social media, web-based sales) as a means of competing with larger competitors also requires these producers to assess the food safety risks associated with being online. Cyberbiosecurity has emerged as a new framework for addressing these specific types of hazards. Small fermentation businesses are encouraged to learn the basics of cyberbiosecurity, how to identify smart technology and automation in their own businesses and identify ways to protect their operations.

Cyberbiosecurity threats can happen to any small fermentation business. As Tamang et al., 2020 points out, fermented food items are generally considered safe, but improper fermentation of those foods can lead to health risks. A cyberbiosecurity attack could easily cause the improper fermentation of a food item, either by affecting the parameters within which the fermentation process is occurring (e.g., temperature sensors) or by affecting the sanitation and hygiene of the automated equipment (e.g., CIP systems).

What is Cyberbiosecurity?

With the increasing use of smart technology and automation in the fermentation industry, the relevance of cybersecurity has been rising too. Cyberbiosecurity is widely applicable to various industries, so guidance should be specifically tailored to an industry. Cyberbiosecurity exists at the intersection of biosecurity, biosafety, and cybersecurity (Figure 1). It is “a formal new enterprise which encompasses cybersecurity, cyber-physical security and biosecurity as applied to biological and biomedical-based systems,” (Duncan et al.,2019).

- Cybersecurity is focused on the protection of data, information systems, and networks (Murch et al., 2018).
- Biosecurity is focused on preventing hazards, or minimizing the hazards that can harm humans, animals, or the environment.
- Biosafety is focused on the prevention of loss of integrity biologically, environmentally and in relation to human health.

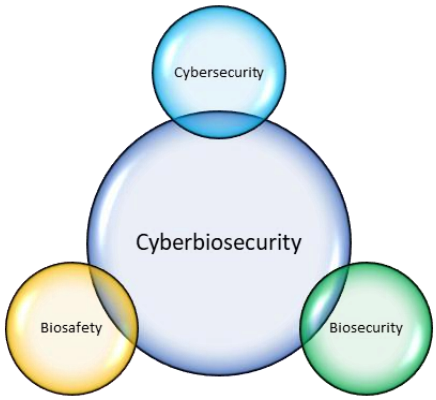

Figure 1. Cyberbiosecurity is the intersection of cybersecurity, biosafety, and biosecurity.

Smart Technology and Automation

There are two terms relevant to cyberbiosecurity hazards in modern small fermentation businesses:

- "Smart Technology" is the utilization of electronic devices connected to a wireless network, capable of logging and reports, or can be programmed to be automated to do a job for the operator, such as receiving alerts to your phone or computer should the power to a piece of equipment be interrupted.

- "Automation" is the utilization of technology to perform otherwise human activities with or without human assistance, such as automatic bottle fillers.

Relevance to Fermentation

Automation within the fermentation industry can be as simple as introducing an automatic temperature controller or an auto-stop valve on a piece of equipment (Pyke, 1959). Even these simple pieces of automation could be the mode of action in a cyberbiosecurity attack and impact the fermentation process. Furthermore, all that is required for these attacks to occur is for the perpetrators to gain access to business control systems (such as through unprotected internet networks) and understand how to change the settings of smart technology or automated devices. These attacks are likely to go unreported or underreported due to a lack of detection, either in the hardware or software of these smart technologies and automated systems (Drape et al., 2021).

Cyberbiosecurity and Hazard Prevention Tools

Hazards are "any biological, chemical, or physical agent that is reasonably likely to cause illness or injury in the absence of its control" [21 CFR § 120.3(g)]. Like the other hazard types (biological, chemical, physical), the manufacturing process should be evaluated for areas where cyberbiosecurity threats can occur. It is highly recommended that cyberbiosecurity hazards be added to hazard prevention tools, like HACCP (Hazard Analysis and Critical Control Point) Programs. Once identified, those areas can be analyzed for the level of risk to the product, what controls are in place to prevent a cyberbiosecurity attack, what would occur in the event of a cyberbiosecurity attack, what the Critical Control Point (CCP) would be, and any corrective measures needed.

Some protective measures that can be built into your business and hazard plans are:

- Separating your home and business technology by using separate computers and network linked technology for home and business
- Avoiding performing business on an unprotected home or public network
- Using passwords and 2-factor authentication on any smart technology or automated processes
- Limiting or excluding access to smart technology or automated processes to a small number of trained employees
- Utilizing security software on all smart technology and automated processes
- Using dataloggers with alerts built in for when specific parameters or controls are not met
- Training employees to be aware of cyberbiosecurity attacks and what they may look like, as you would for other types of hazards

Recommendations

- Businesses should separate their business networks from unprotected home networks and devices. Home networks are less likely to be as strongly protected against a cyberbiosecurity attack as a protected business network would be.
- It is imperative to have at least a base level knowledge of the technology being used, what automation is taking place, and basic protection measures for those items.

- Senior management should prioritize education about cyberbiosecurity through free classes on the internet, paid courses through a college, etc.
- If possible, it can be incredibly beneficial to perform an internal hacking event to identify weaknesses within the cyber realm of your business. This can make curating cyberbiosecurity protections personal to your business.

References

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 in Bioengineering and Biotechnology*, *9*. https://doi.org/10.3389/fbioe.2021.737927

Duncan, S. E., Reinhard, R., Williams, R. C., Ramsey, F., Thomason, W., Lee, K., Dudek, N., Mostaghimi, S., Colbert, E., & Murch, R. (2019). Cyberbiosecurity: A new perspective on protecting U.S. food and agricultural system. *Frontiers in Bioengineering and Biotechnology*, *7*(MAR). https://doi.org/10.3389/fbioe.2019.00063

Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy. *Frontiers in Bioengineering and Biotechnology*, *6*(APR). https://doi.org/10.3389/fbioe.2018.00039

Pyke, M. (1959). Automation and the fermentation industries. *Journal of the Institute of Brewing*, *65*(3), 239–246. https://doi.org/10.1002/j.2050-0416.1959.tb01451.x

Tamang, J. P., Cotter, P. D., Endo, A., Han, N. S., Kort, R., Liu, S. Q., Mayo, B., Westerik, N., & Hutkins, R. (2020). Fermented foods in a global age: East meets West. *Comprehensive Reviews in Food Science and Food Safety*, *19*(1), 184–217. https://doi.org/10.1111/1541-4337.12520

Visit Virginia Cooperative Extension: ext.vt.edu

2022 VCE-000NP