Cyberbiosecurity Importance in Relation to Small Fermentation Businesses and How to Integrate it into Known Hazard Prevention Tools

Jordan Nicole Reisterer Knapp

Major Project and Report submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of

Online Master of Agricultural and Life Sciences
In
Food Safety and Biosecurity

Dr. Laura K. Strawn, Department of Food Science and Technology
Dr. Joseph Eifert, Department of Food Science and Technology
Dr. Alexis M. Hamilton, Department of Food Science and Technology
Brian Wiersema, Department of Food Science and Technology

(Date of Submission – 08/07/2024)

Keywords: cyberbiosecurity, food safety, hazard prevention, fermentation

Cyberbiosecurity Importance in Relation to Small Fermentation Businesses and How to Integrate it into Known Hazard Prevention Tools

Jordan Nicole Reisterer Knapp

ABSTRACT

Cyberbiosecurity threats are on the rise in many various industries. With attacks on water treatment plants, medical facilities, and more, awareness for what cyberbiosecurity is, what it looks like, and how to implement countermeasures into known hazard prevention tools is dire.

This project set out to address these issues in the context of small fermentation businesses. A survey was conducted to better guide how a factsheet would be created and used to gauge, what the fermentation community in North Carolina and Virginia was aware of in relation to food safety, the Food Safety Modernization Act, and cyberbiosecurity.

A factsheet was designed to guide small fermentation businesses on how to identify what cyberbiosecurity is, how to implement control measures into known hazard prevention tools, and what methods exist to better protect their businesses.

Table of Contents

Introduction

Background and Setting

Cyberbiosecurity threats are on the rise in many various industries (Drape et al., 2021). With attacks on water treatment plants, medical facilities, and more, awareness for what cyberbiosecurity is, what it looks like, and how to implement countermeasures into known hazard prevention tools is dire. This project sets out to address these issues in the context of small fermentation businesses. While it may not seem as if these businesses will be a target of a cyberbiosecurity attack, the ones carrying out these threats can have a variety of targets. Attacks on smaller entities are known to be far more successful than mass scale attacks. It is important to acknowledge and support these smaller businesses and industries when possible.

Statement and Significance of Problem

The main concern of this project is that cyberbiosecurity awareness is low in most industries, including the fermentation community (Drape et al., 2021). As cyberbiosecurity threats increase within the realm of food production and adjacent industries (Drape et al., 2021), creating awareness and educational documents specific to various industries can aid in the ablation of these threats or prevent them in the first place.

Purpose of Project

The objective of this project was to create a factsheet for small fermentation businesses to use to learn what cyberbiosecurity is, the importance of cyberbiosecurity awareness within these businesses, and how to implement cyberbiosecurity measures into known hazard prevention tools, such as HACCP planning, SOPs, cGMPs, or any other tool the business may be using to manage food safety hazards.

Definition of Keywords and Terms

1. *Hazards:*
    a. *Cyber:* hazards, relative to, but not solely in regards to food safety, that arise from the failure of technologies used by the facility by unauthorized access or misuse (i.e. hacking, data breaches, etc.)
    b. *Chemical:* hazards that arise from chemical substances that are naturally occurring or are added to food products that can cause harm or food borne illness (i.e. pesticides, antibiotics, toxins, etc.)
    c. *Biological:* hazards that arise from living organisms (i.e. bacteria, fungi, etc.)
    d. *Physical:* hazards that arise from foreign materials that can cause injury or contamination (i.e. rocks, glass, plastics, etc.)
2. *FDA:* Food and Drug Administration
3. *Current Good Manufacturing Practices (cGMPs*): regulations enforced by the FDA in relation to the design, monitoring, and control of the manufacturing process.
4. *Critical Control Points (CCPs):* the points at which controls can be implemented to prevent, eliminate, or reduce a food safety hazard to acceptable levels.
5. *Hazard Analysis and Critical Control Point (HACCP) programs:* a management system used to monitor a food system by identifying, managing and controlling food safety hazards to safe and acceptable levels.
6. *Food Safety Modernization Act (FSMA):* signed into law in 2011 that authorizes the FDA to regulate how foods are grown, processed and harvested.

7. *Standard Operating Procedures (SOPs):* written protocols and procedures designed to facilitate the standardization of operations within a facility in regard to regulations, safety, replicability, etc.
8. *Preventive Controls (PCs):* controls whose purpose is to prevent the occurrence of errors through the separation of duties.
9. *Smart Technologies:* 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.
10. *Automation:* the utilization of technology to perform otherwise human activities with or without human assistance
11. *Cyberbiosecurity:* "a formal new enterprise which encompasses cybersecurity, cyber-physical security and biosecurity as applied to biological and biomedical-based systems," or "understanding the vulnerabilities to unwanted surveillance, intrusions, and malicious and harmful activities which can occur within or at the interfaces of comingled life and medical sciences, cyber, cyber-physical, supply chain and infrastructure systems, and developing and instituting measures to prevent, protect against, mitigate, investigate and attribute such threats as it pertains to security, competitiveness and resilience." (Murch et al., 2018)
12. *Fermentation:* the process by which microorganisms break down carbohydrates into energy anaerobically and/or in the absence of oxygen; used commercially to produce various food and drink products and as a method of preservation.
13. *Small Business:* a business with a small number of employees and small operation capacity.

14. *Registered Food Facility:* Domestic and foreign facilities that manufacture, process, pack, or hold food, for human or animal consumption in the United States registered with the FDA, per the requirements of the Food Safety Modernization Act and the Public Health Security and Bioterrorism Preparedness and Response Act of 2002.
15. *QuestionPro©*: a survey software approved for use by Virginia Tech

Literature Review

Food Safety, Hazards, and Planning Tools

Food safety is a concern that touches on many aspects of life: food production, food consumption, consumer health, economies, international trade and more. Knowledge surrounding food safety is actively changing and adapting in the modern age and the approaches to handling food safety concerns are changing as new threats arise. Food safety threats are traditionally known as hazards. The four main categories of hazards are biological, physical, chemical and cyber, with cyber hazards holding the least amount of focus. To manage these potential threats and control hazards present in the food production process many prevention and planning tools are available to food producers. Some of these tools are voluntary, while others are mandated by the Food and Drug Administration (FDA) with the Food Safety Modernization Act of 2011 (FSMA).

For general background, FSMA was enacted by Congress in 2011 in response to an increasing rate of foodborne illness outbreaks in the United States. FSMA brought power to the FDA to change the landscape of food safety from reactive to preventive (Strauss, 2011). This meant that the FDA wanted to now prevent food safety hazards and outbreaks before they occurred instead of reacting to outbreaks after they already happened. While prevention is the theme of FSMA, it also focuses on FDA inspections and compliance, food safety for imports, response measures, and partnerships (Strauss, 2011).

With prevention in mind, FSMA requires that, through current good manufacturing practices (cGMPs), food facilities have a food safety plan. This plan has to include a risk-based analysis of any potential food safety hazards and the preventive controls (PCs) to be used to minimize said hazards. While cGMPs are required, whether a

facility is registered or not with the FDA, specific hazard prevention tools are voluntary. The most well-known of these hazard prevention tools is Hazard Analysis and Critical Control Point planning (HACCP), a management system used to monitor a food system by identifying, managing and controlling food safety hazards to safe and acceptable levels (Ropkins & Beck, 2000). Critical control points (CCPs) are the points at which controls can be implemented to prevent, eliminate, or reduce a food safety hazard to acceptable levels (Unnevehr & Jensen, 1998). HACCP is used to identify a hazard, identify when and where it occurs, why it occurs, at what point the hazard is critical (CCP), and analyzes how to reduce, prevent, and monitor the hazard and how to correct the occurrence of the hazard should the approved procedures fail. HACCP is often then used to guide standard operating procedures (SOPs) for the food facility, written protocols and procedures designed to facilitate the standardization of operations within a facility in regard to regulations, safety, replicability, etc.

Consequently, even with all the aforementioned safety regulations and planning tools, FSMA and HACCP have aged, and the current landscape globally, nationally, and locally are actively advancing and changing. There is a modern hazard that is not included in FSMA and HACCP, cyberbiosecurity.

Cyberbiosecurity Applicability to Fermentation Businesses

With the increasing use of smart technology and automation on the rise in the food production industry, the relevance of cybersecurity has been rising too. The intersection of food safety, biosecurity, biosafety, and cybersecurity was not previously recognized as a unique hazard. Biosecurity is focused on preventing the hazards, or minimizing the hazards that can harm humans, animals, or the environment.

Cybersecurity is focused on the protection of data, information systems, and networks (Murch et al., 2018).

Cyberbiosecurity threats can come in many different forms, broadly being access to systems, data, or technologies with the intent to harm (Duncan et al., 2019). Furthermore, the actors of these attacks have little need to know how food production occurs or works, just the technical aspects of how to make the technology not do what it was set up and intended to do. 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).

With cyberbiosecurity being such a new topic and with it being broadly applicable to many different aspects of the food industry, it is hard to narrow down specific protections against attacks. Drape et al., 2021 identified that training and classes need to be offered on cyberbiosecurity, but it is unclear who would currently be qualified to teach these courses. There is also the option to incorporate cyber hazards into HACCP planning. As of now, HACCP focuses on biological, chemical, and physical hazards, not cyber. Both options have promise but need to be specific and applicable to the industry audience they address.

Murch et al., 2018 stated that "because of its diversity and extent, cyberbiosecurity needs its own systematics, so that it can be better communicated, organized, explored, advanced and implemented." Cyberbiosecurity is so open ended and can apply to many different realms, there needs to be guidelines and information given in ways that are relevant to each various sphere. As guidance has grown in relation to cyberbiosecurity awareness, not much has been given to the fermentation industry, let alone smaller fermentation 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. Twenty percent of small businesses have been hacked (Duncan et al., 2019). This statistic shows that cyber-attacks are not limited to larger businesses and corporations, as many smaller businesses may assume. This is further supported by Drape et al., 2021 who found in a case study that there is a mindset of "this doesn't involve me… I do not handle technology, so I don't need to deal with it."

Cyberbiosecurity threats can happen to any of these small fermentation businesses. 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 or by affecting the sanitation and hygiene of the automated equipment.

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 cause issues in the fermentation process, such as leading the fermentation to occur at the wrong temperature, leading to the growth of harmful organisms or causing too little of a sanitation liquid into the equipment needing to be sanitized. This is further compounded by the fact that some fermented products are only produced in one specific geographic area. If an attack were to occur to these businesses, the global supply of that item could be affected. An example of this would be natto, a *bacillus* fermented soybean food, which is only produced in the 'natto-triangle' of China,

Japan, Thailand, Korea, and Northern India (Tamang et al., 2020). All of these concerns are why this project is being conducted.

Project Methodology and Design

Targeted Audience

The audience of this project is small fermentation businesses with an interest in learning what cyberbiosecurity is, why it is important, and how to implement it into their hazard prevention tools.

Methodology

The initial methodology of this project was to create a survey to query the fermentation community in Virginia and North Carolina on their awareness of food safety hazards, food safety regulation, food safety hazard preventive measures, cyberbiosecurity and the role of the survey taker within their specific fermentation business, and what area of fermentation the business produces within (i.e. cidery, winery, brewery, etc.). The survey was created, approved for exemption by the Virginia Tech Institutional Review Board (IRB #23-1054), and released on QuestionPro© on October 1st, 2023. Survey questions can be found in Appendix A.

The survey was released for several months on a private invite basis through many different fermentation contacts and groups. After low interaction and response rate, the survey was opened to the public on February 22nd, 2024. Interaction and response rate did not increase, nor did survey results change. The survey was closed on May 19th, 2024 (n = 3-12 responses).

Upon review of the information and responses received, it was determined that a deeper literature review would be conducted, and responses would be analyzed in a qualitative and colloquial manner to better guide how the factsheet would be constructed.

Summary of Outcomes, Discussions, and Recommendations

Outcomes and Results

Due to low response rate, there was no statistical nor quantitative analysis performed on the survey results. The information discussed next was used to better guide how the factsheet was created and to gauge what the fermentation community in North Carolina and Virginia was aware of in relation to food safety, FSMA, and cyberbiosecurity.

Fifty percent of the respondents operated in both North Carolina and Virginia, with a wide representation of fermentation business type and where the respondents worked within the business. These businesses represented were a brewery (2), cidery (1), winery (1), goat cheese (1), and various raw materialists (3). Within these businesses the respondents worked in management (2), production (2), quality control or analysis (2), sales (2), research and development (2), finance (1), and human resources (1). Sixty percent of respondents were registered food facilities with the FDA, while 20% were not, and the rest were unsure. One hundred percent of respondents had taken some form of food safety training.

In relation to the food safety and cyberbiosecurity awareness section, response rate was significantly lower than the demographic section. There were three consistent respondents, with an occasional fourth. Fifty percent of respondents were able to identify all four hazard types, 40% were able to identify biological, chemical, and physical hazards, and 10% were able to identify only biological hazards. Fifty percent of respondents used hazard prevention tools, while 75% had written safety protocols, cGMPS, or standard operating procedures. All respondents were aware of FSMA.

Lastly, 50% of respondents were unsure of if their business utilized smart technology or automation, while the other 50% did not. All respondents utilized some form of control in relation to smart technology or automation. This was in the form of passwords (1), 2-factor authentication (1), limited or exclusionary access (1), or other security software (1). Two respondents were aware of what cyberbiosecurity is, while the other was unsure. When asked if respondents would like more information on cyberbiosecurity, 5/6 responded yes.

Implications, Impacts, and Recommendations

Boys et al., 2015 spoke to how foodborne illness costs the U. S. economy around 14 billion dollars each year. With cyberbiosecurity threats and attacks on the rise (Drape et al., 2021), this number is bound to increase; hence, why better protections are needed. These protections need to be individualized and specific to the different industries involved.

For the small fermentation businesses surveyed and spoken for in this project, there are a few recommendations to be made. While respondents were limited within the survey, many responded with an interest in cyberbiosecurity (5), and some already had some background knowledge (2). With the basic cyber controls already being used, there is room for improvement.

To start, it needs to be acknowledged that small fermentation businesses are not safe nor excluded from cyberbiosecurity attacks. As mentioned above, 20% of small businesses have been hacked (Duncan et al., 2019). This is why it is recommended that businesses separate their businesses from home networks and devices. Home networks are less likely to be as strongly protected against a cyber-attack as a business network would be.

Secondly, 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. However, it is harder for a small business to have the capital to maintain a dedicated information technology team or person (Drape et al., 2020). They may need to take on this role themselves. This can be done 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 the business. This can make curating cyberbiosecurity protections personal to the business.

Lastly, it is highly recommended that cyberbiosecurity hazards be added to hazard prevention tools, like HACCP. Like the other hazard types, the manufacturing process should be evaluated for areas where cyber threats can occur. 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 CCP would be, and any corrective measures needed.

Dissemination Plan

To disseminate the recommendations and information gleaned from this project an educational factsheet on cyberbiosecurity for small fermentation businesses was created and can be found in Appendix B. This factsheet will be published alongside this report, freely available through Virginia Cooperative Extension.

References

Boys, K. A., Ollinger, M., & Geyer, L. L. (2015). The food safety modernization act: Implications for U.S. small scale farms. In *American Journal of Law and Medicine* (Vol. 41, Issues 2–3, pp. 395–405). SAGE Publications Inc. https://doi.org/10.1177/0098858815591524

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

Ropkins, K., & Beck, A. J. (2000). *Evaluation of worldwide approaches to the use of HACCP to control food safety*.

Strauss, D. M. (2011). An Analysis of the FDA Food Safety Modernization Act_ Protection. *". Food and Drug Law Journal 66.3*, 353–376.

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

Unnevehr, L. J., & Jensen, H. H. (1998). *The Economic Implications of Using HACCP as a Food Safety Regulatory Standard*.

Appendices

Appendix A- Survey Questions

This survey is protected by Respondent Anonymity Assurance. Respondent Anonymity Assurance (RAA) is a principle that aims to protect the identity of the survey participants so that they can give honest answers without worrying about the repercussions. Respondent email, IP address, Country code, nor region will be collected. For further details on RAA, please click the red text link on the bottom right-hand side of the survey. This survey is being provided to your business to help Virginia Tech researcher, Jordan Knapp, gauge the knowledge of food safety and cyberbiosecurity within the fermentation communities of North Carolina and Virginia. Your responses to this survey, on behalf of your business, will help Mrs. Knapp create important educational documents for the fermentation community, educating on the concept of cyberbiosecurity and/or help provide other resources from Virginia Tech in regard to food safety. Your participation is important, and all responses are beneficial. Thank you for your time and effort and should you wish to receive the finalized informational documents, once the project is complete, there will be a place at the end of the survey to request so.

Which area of fermentation is your business?

1. Brewery
2. Cidery
3. Winery
4. Distillery
5. Meadery
6. Raw Materials: Maltster, Grain, etc.
7. If none of these, how would you describe it? _____

Which state does your business operate in?

1. North Carolina
2. Virginia
3. Both
4. Other _____

What role do you play in your facility?

1. Management
2. Production
3. Quality Control & Analysis
4. Sales
5. Research & Development
6. Finance
7. Human Resources
8. Other _____

Is your facility a registered food facility with the FDA? Defined as: Domestic and foreign facilities that manufacture, process, pack, or hold food, for human or animal consumption in the United States, registered with the FDA, per the guidance of the Food Safety and Modernization Act and Bioterrorism Act.

1. Yes
2. No
3. Unsure

Have you/ others in your facility encountered any food safety training or attended a course where food safety was discussed? (food safety, food safety hazards, cGMPs, etc.)

1. Yes
2. No

Can you/ could you identify a food safety hazard of each of these types?

1. Physical: hazards that arise from foreign materials that can cause injury or contamination (i.e. rocks, glass, plastics, etc.)
2. Chemical: hazards that arise from chemical substances that are naturally occurring or are added to food products that can cause harm or food borne illness (i.e. Pesticides, antibiotics, toxins, etc.)
3. Biological: hazards that arise from living organisms (i.e. bacteria, fungi, etc.)
4. Cyber: hazards that arise from the failure of technologies used by the facility by unauthorized access or misuse (i.e. hacking, data breaches, etc.)

Do you/ your facility have Current Good Manufacturing Practices? (cGMPs) or Standard Operating Procedures (SOPs)/ written protocols?

1. Yes- cGMPs
2. Yes- SOPs/ written protocols
3. Both cGMPS and SOPs/ written protocols
4. No
5. Unsure

Do you/ your facility use food safety hazard planning tools? (i.e. like HACCP- Hazard Analysis and Critical Control Points, or PC- Preventive Controls)

1. Yes
2. No
3. Unsure

Is your facility aware of The Food Safety Modernization Act and how it applies to fermentation products and facilities?

1. Yes
2. No
3. Unsure

Does your facility use smart technologies/ automation? Defined as: Smart technologies can be 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 you.

1. Yes
2. No
3. Unsure

What controls does your facility use in relation to electronic record keeping, automation parameters, etc.?

1. Passwords/ two factor authorization

2. Limited access/ exclusionary access
3. Various security software(s)
4. Datalogging with alerts
5. Other_ select this box and record your method type _____

Are you aware of what cyberbiosecurity is?

1. Yes
2. No
3. Unsure

Would you like further information on cyberbiosecurity threats? If so, what form would you like this information in?

1. Yes (short module, factsheet or brochure)
2. No
3. If yes, please check this box and record the form you would like the information in. Thank you! _____

If you would like to discuss the topics listed above or receive the finalized informational documents on cyberbiosecurity, please leave an email address below to be contacted at once the project is complete. Thank you!

Appendix B- Cyberbiosecurity for Small Fermentation Businesses Factsheet

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

Cyberbiosecurity for Small Fermentation Businesses:

How to Integrate it into Known Hazard Planning Tools

Authored by Jordan Reisterer Knapp, Graduate Student, Agriculture and Life Sciences, 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. Twenty percent of small businesses have been hacked (Duncan et al., 2019). This statistic shows that cyber-attacks are not limited to larger businesses and corporations, as many smaller businesses may assume. This is further supported by Drape et al., 2021, who found in a case study that there is a mindset of "this doesn't involve me… I do not handle technology, so I don't need to deal with it." So, while you may think an attack may not happen to you, you must acknowledge that it could. With that in mind, this factsheet is here to help guide you in learning the basics of what cyberbiosecurity is, how to identify smart technology and automation, and some recommendations on how to support your small fermentation business.

What is Cyberbiosecurity?

With the increasing use of smart technology and automation on the rise in the food production industry, the relevance of cybersecurity has been rising too. Cyberbiosecurity is the intersection of food safety, biosecurity, biosafety, and cybersecurity. Biosecurity is focused on preventing the hazards, or minimizing the hazards that can harm humans, animals, or the environment. Cybersecurity is focused on the protection of data, information systems, and networks (Murch et al., 2018).

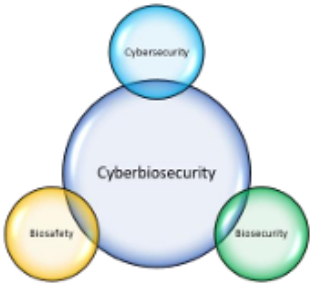

Figure 1. Cyberbiosecurity is the intersection of cybersecurity, biosafety, and biosecurity.

Smart Technology and Automation

- 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.
- Automation is the utilization of technology to perform otherwise human activities with or without human assistance.

Recommendations

- It is recommended that businesses separate their businesses from home networks and devices. Home networks are less likely to be as strongly protected against a cyber-attack as a 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.
- You may need to take on this role yourself or with others in your business. This can be done 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.

Cyberbiosecurity and Hazard Planning Tools

It is highly recommended that cyber hazards be added to hazard planning tools, like HACCP: Hazard and Critical Control Point Analysis. Like the other hazard types, the manufacturing process should be evaluated for areas where cyber threats can occur. Once identified, those areas can be analyzed for the level of risk to the product, what controls are in place to prevent a cyber-attack, what would occur in the event of a cyber-attack, what the CCP would be and any corrective measures needed.

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

- 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 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 cyber-attacks and what they may look like, as you would for other types of hazards: biological, chemical, and physical

Relevance to Fermentation

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, or by affecting the sanitation and hygiene of the automated equipment. 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 cause issues in the fermentation process. Furthermore, the actors of these attacks have little need to know how food production occurs or works, just the technical aspects of how to make the technology not do what it was set up and intended to do. 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).

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