Cyberbiosecurity of Fermentation: Agentic AI and Brewing Resilience

Zachary Lara[1], Xavier-Lewis Palmer[2], Lucas Potter[2] and Jesse Friedman[3]
[1]Independent Researcher, San Francisco, CA, USA
[2]BiosView Labs, Dayton, OH, USA
[3]Brewery Organization and Process Consultant, Los Angeles, CA, USA

zglara@gmail.com (Corresponding authors)
xp.bv@pm.me (Corresponding authors)
jwfriedman@gmail.com (Corresponding authors)

Abstract: Do you know what is in your beer? Increasingly, the answer depends not only on ingredients and fermentation, but on the integrity of the digital and physical systems that govern production. This paper examines commercial brewing as an underdeveloped cyberbiosecurity workforce problem intensified by AI. Brewing increasingly depends on digital networks, automated control, and connected supply chains. Yet the process remains a biologically active process shaped by human judgment, microbial control, and physical equipment. Although cyberbiosecurity research addresses biotechnology, biomanufacturing, food, and agriculture, commercial fermentation has received comparatively limited attention. Brewing is a useful case because cyber incidents can disrupt fermentation, sanitation, packaging, quality control, and operational decision-making even when finished beer remains inhospitable to many pathogens. Malicious use of AI to uplift novice actors, used in conjunction with generative phishing attacks, may further reduce informational barriers and support coordination across cyber, biological, and physical domains, although current evidence does not establish fully autonomous adversarial operations. Drawing on cyberbiosecurity, OT-security, workforce, and training frameworks, this paper identifies a socio-technical gap between brewing science and cybersecurity and proposes a competency model incorporating AI literacy, OT awareness, biological anomaly recognition, and scenario-based training. It argues that workforce preparedness should complement technical and governance controls in securing increasingly digitized brewing environments.

Keywords: Cyberbiosecurity, Agentic AI, Brewing, Fermentation, Workforce education, Operational technology

1. Introduction

Recent incidents demonstrate that cyberattacks on food manufacturers can produce substantial physical and economic disruption. The 2017 NotPetya attack severely disrupted Mondelez International's operations; in 2021, ransomware temporarily shut JBS facilities in the United States, Canada, and Australia; and in 2022, a ransomware incident disrupted manufacturing and distribution at KP Snacks (Manning and Kowalska, 2026). Rather than demonstrating operational-technology compromise in every case, these incidents establish a recurring capacity for attacks on digital systems to interrupt physical food production and supply chains. This paper examines an underdeveloped part of that problem: commercial brewing.

Brewing presents a distinctive cyberbiosecurity case because of the physicochemical properties of finished beer including ethanol, low pH, carbon dioxide, nutrient limitation, and antimicrobial hop compounds. The ethanol, pH, and carbon dioxide specifically make it inhospitable to many microorganisms, including many human pathogens (Bokulich and Bamforth, 2013; Raihofer et al., 2022). Yet microbial stability of the finished product does not make the production system secure. Beer-adapted spoilage organisms can persist under conditions that inhibit many other microorganisms and can produce consequences including over-attenuation, altered sensory characteristics, excess carbonation, and package failure (Meier-Dörnberg et al., 2018). Intentional biological contamination of food also has historical precedent: the 1984 Oregon salmonellosis outbreak demonstrated that deliberate contamination could cause widespread harm while initially resembling a conventional foodborne event (Török et al., 1997). In brewing, however, malicious biological interference need not involve a human pathogen or cause illness to be consequential. Brewing therefore presents a security asymmetry: a product comparatively resistant to conventional foodborne pathogens remains dependent on a biologically active production process in which yeast performance, microbial exclusion, temperature control, cleaning and sanitation, packaging integrity, quality records, sensory evaluation, and coordination between digital and physical systems determine production outcomes. A malicious cyber or cyber-physical incident need not poison consumers to impose harm; interference with process parameters, records, logistics, contamination detection, or quality-control functions could instead degrade product, interrupt production, or delay recognition of abnormalities.

Cyberbiosecurity provides an appropriate framework for examining this convergence. Murch et al. (2018) position the discipline at the interface of cybersecurity, cyber-physical security, and biosecurity, while

Richardson et al. (2019) emphasize cooperation among life-science, information-technology, and security communities. Duncan et al. (2019) extends this perspective across food and agriculture, identifying vulnerabilities spanning production, transportation, suppliers, retailers, and consumers. Potter and Palmer (2023) further emphasize the importance of mission-directedness and the bidirectional movement of risk between biological and digital domains. Within this literature, however, commercial fermentation and particularly the workforces operating at the boundary between biological processes and digitized production has received comparatively little explicit treatment. We explore this deficit of workforce education and training, within this paper, providing some suggestions for remedy.

AI-enabled systems may further alter this risk by reducing some of the informational and expertise barriers that historically separated cyber and biological domains. Industrial-control-system (ICS) attacks such as Stuxnet and Triton illustrate the complexity of multi-stage operations requiring specialized understanding of both digital systems and physical processes (Langner, 2011; Kumar et al., 2022; Firoozjaei et al., 2022). Stuxnet, in particular, represented an unusually sophisticated effort to translate manipulation of industrial-control logic into physical process effects, while analyses of Stuxnet and Triton characterize such campaigns as strategic, multi-stage attacks against complex industrial environments. Contemporary LLMs do not remove these requirements, but they may change how specialized knowledge is accessed and combined. Soice et al. (2023), for example, show that LLMs can assist non-specialists in locating and organizing dual-use biological information, while Mouton, Lucas and Guest (2023) examine the operational risks associated with LLM assistance in biological-attack planning and Hattoh et al. (2025) further investigate the biological-design capabilities of contemporary language models. In cybersecurity, LLMs are likewise being examined for vulnerability reasoning, attack-related tasks, and increasingly automated post-breach workflows (Xu et al., 2024a; Xu et al., 2024b).

These developments should not, however, be interpreted as evidence that AI has eliminated expertise requirements or can autonomously sustain complex adversarial operations over extended periods. RAND's subsequent red-team study found no statistically significant improvement in the viability of biological-attack plans produced with LLM assistance compared with those developed without such assistance (Mouton et al., 2024). The more defensible concern is therefore not the collapse of the expertise barrier, but its potential reduction: AI may make fragmented knowledge easier to locate, synthesize, and coordinate across domains. In a brewing context, this raises the possibility that knowledge of OT systems, fermentation biology, vendor documentation, social engineering, quality-control practices, and supply-chain timing could be assembled more readily into a coordinated attack concept. This represents a plausible coordination effect rather than evidence that present AI systems can independently execute such campaigns.

Emerging defensive research reinforces the need to treat this as a layered socio-technical problem. BioShield, for example, proposes a context-aware application-level firewall combining domain-specific prompt-risk assessment with post-generation verification to constrain harmful or dual-use outputs from biological LLMs (Das et al., 2026). The Biosecure-LLM framework extends this discussion from technical filtering to governance, arguing that domain-specific policy enforcement should be separable from model inference and implemented through independently auditable control layers rather than residing solely within model providers (Palmer et al., 2026). These approaches demonstrate that model- and application-level safeguards are becoming more specialized, but they also illustrate the limits of treating cyberbiosecurity solely as a model-security problem. Neither model filtering nor external AI-governance mechanisms can independently secure the production environment in which digital systems interact with microorganisms, physical equipment, process conditions, and human operators.

This makes commercial brewing a technical-security problem, as well as an education and workforce-policy problem. Existing cyberbiosecurity workforce research identifies limited educational opportunities and emphasizes interdisciplinary preparation spanning biological, information-technology, and operational-technology contexts (Adeoye et al., 2023). This evidence does not establish a brewing-specific education deficit, but it provides a broader basis for examining whether comparable gaps exist within commercial fermentation. The scale of the sector makes the question consequential: global beer consumption alone reached approximately 194 million kilolitres in 2024 (Kirin Holdings Company, 2025). Workers positioned closest to production anomalies, including packaging operators, cellar technicians, brewers, quality analysts, and maintenance personnel, operate where biological processes intersect with increasingly digitized production systems. We therefore identify a potential socio-technical blind spot: if brewing science and cybersecurity are taught and practiced as separate domains, frontline personnel may lack a shared framework for distinguishing routine process variation from malicious or AI-assisted interference. Addressing this gap requires technical

safeguards, organizational governance, and workforce education to be treated as complementary components of cyberbiosecurity rather than as separate problems.

2. Agentic AI and the Cyber-physical Frontier

Agentic AI differs from conventional task automation in its capacity to pursue goals through combinations of planning, tool use, environmental interaction, memory, and iterative adaptation (Acharya, Kuppan and Divya, 2025). In cyber-physical environments, these capabilities are relevant in four related ways: they may reduce expertise barriers, increase the continuity and tempo of AI-assisted workflows, facilitate cross-domain integration, and support more adaptive attack activity.

First, AI may reduce expertise barriers without eliminating the need for expertise. A malicious actor need not personally master every domain implicated in a cyber-physical incident if an AI system can assist in locating, translating, and organizing information across industrial networking, brewery operations, cleaning-in-place procedures, yeast physiology, vendor documentation, social engineering, and attack timing. This does not mean that a novice can reliably execute a sophisticated operation; rather, the cost of moving from limited knowledge toward a minimally structured plan may decline. Soice et al. (2023) demonstrate a related effect in dual-use biotechnology, where LLMs supplied non-specialists with specialized information, protocols, troubleshooting guidance, and information about external service providers. Mouton, Lucas and Guest (2023) similarly examine whether LLMs could bridge information gaps relevant to biological-attack planning.

Second, AI-assisted workflows may reduce some of the coordination and continuity costs associated with extended operations. Agentic systems can retain intermediate information, summarize reconnaissance, compare observations, generate communication variants, and revisit earlier decisions as new information becomes available. These capabilities do not establish that present systems can autonomously sustain sophisticated attacks over long periods, but they may allow portions of reconnaissance, planning, and monitoring to proceed with less continuous human attention. In brewing, this matters because production, sanitation, fermentation, packaging, maintenance, and distribution operate according to recurring but asynchronous schedules. An adversary able to preserve and integrate observations across these cycles may identify opportunities that are not visible within a single event or shift.

Third, AI may facilitate cross-domain integration. NIST SP 800-82 Revision 3 defines operational technology as systems and devices that interact with or control the physical environment and emphasizes that OT security must account for performance, reliability, and safety requirements distinct from conventional information technology (NIST, 2023). Brewing exemplifies this convergence because biological processes, sensors and controllers, business systems, physical equipment, and human judgment operate as an interdependent production system. AI systems may assist users in connecting information that would otherwise remain separated across disciplinary boundaries. The same capability can aid defenders, but only where organizational structures and training enable personnel to recognize and investigate cross-domain anomalies.

Fourth, AI may support incremental automation and adaptation within cyberattack workflows. Research already explores LLM-assisted vulnerability analysis, malware and phishing tasks, threat analysis, and post-breach automation (Xu et al., 2024a; Xu et al., 2024b). Emerging operational evidence suggests that some of these capabilities are appearing in practice. Dream Research Labs (2026) reported a four-day campaign against government entities in Asia in which a Hermes/OpenClaw multi-agent framework parallelized tasks, preserved operational context, reprioritized attack chains, and sought alternatives when blocked. Taiwan's Administration for Cyber Security subsequently confirmed related attacks involving hybrid human–AI-agent operations (Administration for Cyber Security, 2026). These cases do not demonstrate fully autonomous attackers, but they suggest that discrete attack tasks can increasingly be parallelized, automated, and adapted to changing conditions. In brewing, this matters because digital interference may propagate across biological, physical, and human processes, affecting fermentation, sanitation, packaging, quality assessment, or operator decision-making.

Existing standards address important parts of this environment but do not themselves create a fermentation-specific workforce pathway. NIST SP 800-82 Revision 3 provides guidance for securing OT systems that interact with physical processes (NIST, 2023), while the IEC 62443 family addresses organizational and technical cybersecurity requirements for industrial automation and control systems (IEC, 2024). The NICE Framework provides a common language for cybersecurity Tasks, Knowledge, and Skills and supports sector-specific education, training, and workforce development (NIST, 2020). Adjacent cyberbiosecurity research reinforces the importance of the human dimension: in healthcare, Barnett et al. (2024) identify inadequate staff security

awareness among vulnerabilities associated with increasingly connected infrastructures and include end-user awareness among relevant mitigation measures. Potter and Palmer (2021) further propose biocybersecurity wargaming as a mechanism for organizational learning and for identifying vulnerabilities across digitally connected bioprocessing environments. For brewing, this suggests that sector-specific translation could extend beyond curriculum content to scenario-based exercises and operational drills, in which personnel learn to recognize anomalies spanning biological processes, digital systems, physical equipment, and human decision-making. These frameworks and practices must therefore be adapted to the operational and learning environments of breweries, brewing schools, laboratories, packaging teams, quality functions, and maintenance departments if workers are to recognize cyberbiosecurity as part of normal production competence rather than as a separate specialist concern.

3. Commercial Brewing as a Cyber-physical Biological System

Commercial brewing is an instructive cyberbiosecurity case because it is simultaneously resilient and fragile. Beer has been produced for millennia, and fermentation practices have long relied on empirical control of microbial activity. Modern brewing, however, is where the cyber, biological and physical components introduced in Section 2 converge as everyday infrastructure: enterprise ordering, sensor-driven process control, laboratory databases, packaging automation and logistics software all now mediate a fundamentally biological process. The microbiology of brewing distinguishes it from ordinary manufacturing. Bokulich and Bamforth (2013) describe beer as a microbial product whose quality is shaped by activity across malting and brewing. While selected Saccharomyces strains perform desired fermentation, unwanted bacteria and wild yeasts can affect flavor, stability, attenuation, carbonation and shelf life. Raihofer et al. (2022) situate brewing history within the long development of alcoholic fermentation and yeast technology. The interpretive challenge is to distinguish ordinary variation from quality drift, contamination, process failure or malicious interference.

One central asymmetry can be called the antimicrobial-environment inversion. Finished beer may be hostile to many pathogens, but the brewery environment remains vulnerable to organisms that damage product quality, economic value and brand trust. The consumer may be protected while the producer is exposed. If a scenario does not resemble mass food poisoning, it may not attract attention from public-health or biosecurity planners. Yet economically targeted contamination, particularly when combined with cyber manipulation of records or timing, could be devastating.

Spoilage yeasts illustrate the problem. Saccharomyces cerevisiae var. diastaticus has received particular attention because some strains can ferment dextrins left by primary fermentation, causing hyperattenuation, overcarbonation, phenolic off-flavors, gushing or package failure. Meier-Dornberg et al. (2018) examine the spoilage potential and brewing ability of S. cerevisiae var. diastaticus using genetic, phenotypic and physiological characterization. Zhong et al. (2024) note that diastatic strains contribute to secondary fermentation problems and may lead to product destruction and extensive facility decontamination. Brettanomyces presents a different case. In some beer styles it is intentionally used for complex flavor development; in others, its presence is unwanted contamination that may slowly produce perceptible changes. These organisms are not primarily public-health weapons. Their relevance is subtler: they can be attribution-resistant, slow to reveal themselves and entangled with ordinary debates about flavor, style, yeast handling and quality assurance.

As noted above, AI-assisted persistence maps directly onto brewing's own temporal structure, giving an adversary several exploitable rhythms: seasonal releases, distributor deadlines, quality-hold windows and scheduled maintenance. Production batches may take days or weeks. Some beers are conditioned for extended periods. Distribution can outpace microbiological confirmation, especially in smaller breweries without extensive in-house laboratories. Recall and withdrawal decisions may need to occur within days, while contract brewing, hop contracts, distribution agreements and brand commitments may span years. A malicious actor who understands this timing does not need to create immediate visible harm. Delayed degradation may be more damaging because it travels into the market before detection. If quality records, sensor data or communications are also manipulated, the organization may struggle to determine whether the cause was sanitation failure, supplier variability, staff error, software malfunction or deliberate interference.

A second asymmetry concerns expertise. The person most likely to notice early signs of a brewing anomaly may not be the person trained in cybersecurity. A cellar worker may see unexpected gravity drift. A packaging operator may notice overcarbonation or seam anomalies. A sensory panel may detect phenolic or unusual aromas. A brewer may suspect yeast stress or contamination. An IT contractor may see suspicious logins. A quality manager may see inconsistent laboratory data. Unless these observations are connected, the incident remains fragmented. An anonymized stakeholder statement supplied for this study captures the practical

problem: 'The challenge is not just the software; it is that the person watching the fermentation tank does not know what a malicious network packet looks like.' This should not be read as blaming production workers. It indicates a systems-design failure. Organizations have not built enough shared literacy between the people who understand the tank and the people who understand the packet.

The workforce economics of brewing further complicate resilience. Many breweries rely on shift labor, packaging workers, seasonal staff and on-the-job training. Packaging is physically demanding, time-pressured and often lower-paid than brewing or management roles. High turnover in production roles weakens tacit knowledge, reduces continuity and makes it harder to sustain security culture. A brewery may purchase a technical security solution but fail to fund paid training time, wage progression or cross-training between production and quality teams. In that case, cyberbiosecurity becomes another compliance demand placed on workers who have limited power to act.

4. The Education and Credentialing gap

Current educational pathways remain bifurcated: brewing curricula prioritize process, biology, and production management, while cybersecurity focuses on networks, threat detection, and governance. Although cyberbiosecurity requires integrating these fields, this intersection remains largely unformalized within fermentation industries. While leading brewing programs cultivate deep process literacy, they rarely incorporate OT cybersecurity, AI-enabled threat awareness, or cyberbiosecurity governance as core competencies. Conversely, cybersecurity credentials emphasize IT infrastructure, risk management, and forensics; even advanced industrial programs often address OT through energy or manufacturing lenses rather than fermentation-specific biological processes. Cyberbiosecurity education remains nascent and inconsistent. Adeoye et al. (2023) identify a workforce need for education at the cybersecurity-biosecurity nexus, yet existing initiatives typically focus on synthetic biology, laboratory automation, or biomedical systems, leaving brewing relegated to an indirect food-production activity rather than a distinct fermentation workforce environment. This creates an educator-preparation circularity: brewing instructors often lack cyber fluency, while cyber instructors lack biological expertise. Furthermore, workforce-development administrators may struggle to define the specific cross-domain competencies required for fermentation, and small breweries frequently lack the time or budget to articulate their specific cybersecurity needs. This gap extends to public communication. Consumers typically attribute degraded beer to routine issues like spoilage or poor handling, lacking an AI-literacy scaffold to conceptualize sabotage-induced quality manipulation. Consequently, effective crisis communication must distinguish between safety, quality, and malicious causation to avoid public panic. A fermentation-specific cyberbiosecurity credential should not attempt to homogenize roles but rather define boundary-crossing competencies: recognizing cyber-physical anomalies, understanding digital impacts on biological outcomes, interdisciplinary communication, and evaluating AI-generated information. The NICE Framework (NIST, 2020) provides a valuable linguistic foundation for these tasks, provided it is mapped specifically to fermentation roles

5. Comparative International Perspective

International comparison shows that cyberbiosecurity workforce development begins from different institutional foundations. Germany's *Brauer und Mälzer* apprenticeship offers a useful model because the dual vocational system combines workplace training with vocational schooling (BIBB, 2026). Its current training ordinance already includes brewing processes, equipment operation, packaging, hygiene, quality control, process-control technology, and general digital-security competencies (BMWi, 2021). The policy opportunity is therefore to extend an existing occupational framework toward brewing-specific OT cybersecurity, AI literacy, and cyberbiosecurity incident recognition.

The European Union provides a complementary regulatory driver. NIS2 applies cybersecurity risk-management and incident-reporting requirements to in-scope food businesses engaged in industrial production, processing, or wholesale distribution and also requires cybersecurity training for management while encouraging employee training (European Parliament and Council, 2022). This makes cybersecurity competence an organizational responsibility rather than solely an IT function and provides a basis for linking governance obligations to production-level workforce development.

The United States is more decentralized. Perkins V supports career and technical education pathways, while brewing programs, community colleges, cybersecurity training, industry associations, and employers provide separate workforce-development opportunities (U.S. Department of Education, 2026). NIST supplies common cybersecurity and OT frameworks (NIST, 2020; NIST, 2023), but the programs reviewed here do not reveal an

established pathway integrating brewing science, OT cybersecurity, AI literacy, and cyberbiosecurity incident response. This creates an opportunity for modular or stackable training that connects competencies currently taught in separate domains.

International adaptation must also account for local market and cultural conditions. Gomez-Corona et al. (2016) show distinct attitudes and motivations surrounding craft and industrial beer consumption in Mexico, illustrating why European or U.S. assumptions should not be transferred uncritically across contexts. The most transferable model is therefore not a single curriculum, but a competency framework adaptable to local production structures, regulatory capacity, language, supply chains, and producer resources.

6. Toward an Intentional Response

A serious response should begin with a curriculum. The curriculum should be modular, stackable and role-sensitive. A packaging operator does not need the same training as a chief information security officer; a brewer does not need the same training as a penetration tester; a quality analyst does not need the same training as a distributor. However, all need shared concepts. A baseline module should define cyberbiosecurity in fermentation and explain how biological systems, digital systems and industrial operations interact. A second module should cover AI literacy, including the strengths and weaknesses of generative systems, hallucination, automation bias, social engineering and the risks of relying on AI-generated troubleshooting without verification. A third module should introduce OT fundamentals: sensors, controllers, human-machine interfaces, segmentation, remote access, logging, alarms and the difference between IT and OT priorities. A fourth module should cover brewing-relevant biological anomalies: contamination indicators, sensory drift, hyperattenuation, unexpected pressure, pH shifts, gravity deviations and delayed spoilage. A fifth module should teach incident communication: when to escalate, what to document, how to preserve evidence and how to avoid blame-oriented reporting. A sixth module should address ethics and equity, including dual-use information, worker voice and public communication.

The curriculum should be scenario-based but non-operational. It should present defensive vignettes rather than sabotage instructions: an unexpected gravity drop paired with remote-login anomalies; a packaging overcarbonation complaint paired with missing quality records; a vendor email requesting urgent remote access; or an AI-generated troubleshooting memo that conflicts with sensory evidence. Learners should practice asking what biological process is affected, what digital system could influence it, who needs to know, what evidence should be preserved and what action protects product and workers.

Stackable credentials are the second requirement. A plausible model would include three levels. Level 1, Fermentation Cyberbiosecurity Awareness, would be appropriate for production, packaging, quality and maintenance workers. Level 2, Fermentation OT and Bio-Process Security Practitioner, would target brewers, cellar leads, quality managers, maintenance leads and IT/OT staff. Level 3, Fermentation Cyberbiosecurity Coordinator, would prepare individuals to lead incident exercises, coordinate with management, interface with insurers and regulators, and maintain training programs. Credentials could be co-issued by brewing associations and public-sector cybersecurity partners. NIST and CISA would not need to own the credential, but their frameworks could anchor terminology while brewing Organizations ensure biological and operational relevance. Table 1 summarizes this credential structure below.

Table 1: Proposed credential levels and established roles

LEVEL	CREDENTIAL	PRIMARY ROLES	CORE FOCUS
1	**Fermentation Cyberbiosecurity Awareness**	Production, packaging, quality and maintenance workers	Baseline cyberbiosecurity concepts and anomaly recognition
2	**Fermentation OT and Bio-Process Security Practitioner**	Brewers, cellar leads, quality managers, maintenance leads and IT/OT staff	OT fundamentals and bio-process security integration
3	**Fermentation Cyberbiosecurity Coordinator**	Incident leads and cross-functional coordinators	Incident leadership, management liaison, insurer/regulator interface and training oversight

Credential levels are cumulative and stackable; each builds on the competencies of the level below. Source: proposed model, Section 6.

Educator preparation is the third requirement. The circular gap will not close unless instructors are trained together. Joint fellowships should pair brewing scientists, quality professionals, OT security practitioners, cybersecurity educators and workforce-development specialists. A brewing instructor might spend time in an

industrial cybersecurity laboratory; a cyber instructor might work through fermentation, sensory and brewery-cleaning modules; a community-college faculty member might co-design a simulation with a regional brewery. These fellowships should produce open educational resources, assessment rubrics and scenario libraries that small breweries can adopt without hiring consultants.

Cross-sector partnership is the fourth requirement. The food and beverage sector would benefit from a dedicated information-sharing capability focused on fermentation and food production. An F&B information sharing and analysis center or fermentation security working group could collect anonymized incidents, publish advisories, translate OT guidance into production language and coordinate tabletop exercises. The NIS2 model can serve as a governance template even where legal obligations differ. Voluntary adoption in the United States could include management training, incident-reporting protocols, vendor-security expectations and minimum training commitments.

Labor equity is the fifth and often neglected requirement. Cyberbiosecurity education will fail if it is added to low-wage production work without paid time, wage recognition or promotion pathways. The packaging operator who notices an unusual pattern and the cellar technician who escalates a subtle fermentation anomaly are performing security-relevant work. Organizations should recognize this through paid training hours, wage floors for credentialed responsibilities, language-accessible materials and non-punitive reporting cultures. Otherwise, cyberbiosecurity will reproduce existing labor exclusions.

The human-centered competencies at stake are not soft add-ons. Critical thinking, ethical reasoning, adaptability, communication, sensory attention and practical judgement are core defensive controls. Technical systems can detect some anomalies, but brewing remains a domain where human perception matters. A worker who notices an unexpected Brettanomyces-like note, a pattern of overcarbonation or a mismatch between digital records and tank behavior may be the first effective security sensor. This worker's particular behavior hilariously is not craft (beer) nostalgia, but it is instead behavior formed from recognition that biological-digital systems produce ambiguous signals and that trained humans are needed to interpret them.

7. Limitations and Future Work

This study is conceptual and policy-oriented, designed to frame the intersection of agentic AI, cyberbiosecurity, and brewing workforce development. As such, it is subject to several limitations. First, the analysis relies on synthesized stakeholder input and existing literature rather than primary empirical data on actual cyber-physical incidents in breweries. Consequently, while the framework for human-centered competency is theoretically sound, its efficacy in practice remains untested. Second, the focus on commercial brewing, while useful for its complexity, may not fully capture the distinct cyber-physical risk profiles of other fermentation-based industries, such as pharmaceutical manufacturing or biofuel production, which face different regulatory and economic constraints. Third, the proposed reliance on a "human-in-the-loop" security model presupposes an organizational capacity for training, wage progression, and cultural change that may be inaccessible to resource-constrained small and medium-sized enterprises (SMEs). Future work should prioritize the empirical validation of the proposed credentialing model.

Quantitative research could develop metrics to assess the impact of modular AI literacy training on the speed and accuracy of anomaly detection in pilot brewery settings. Furthermore, there is a need to explore the potential for "defensive AI"—specifically, how agentic systems might be designed to act as force multipliers for human operators, rather than solely as vectors for adversary activity. Comparative studies across broader food-biotechnology sectors could also help refine these competencies, determining whether a unified "fermentation cyberbiosecurity" standard is feasible or if industry-specific adaptations are required. Finally, formalizing quantitative risk modeling for AI-assisted threats in OT environments would provide a stronger evidentiary basis for insurance and regulatory policy, moving beyond qualitative risk assessment toward robust, industry-standard metrics.

8. Conclusion

Agentic AI fundamentally alters the cyberbiosecurity risk landscape in commercial brewing by lowering barriers to cross-domain attack coordination, necessitating a shift beyond traditional technical controls toward a human-centered security model. Because brewing operates at the complex intersection of digital systems, operational technology, and biological processes, resilience requires a workforce capable of interpreting cross-domain anomalies—where a digital event can signal a biological risk and vice-versa. Current educational pathways, however, remain siloed between brewing science and cybersecurity, failing to prepare personnel for this unique

convergence. To address this, the industry must adopt an intentional, multi-layered policy response that includes modular curricula, stackable credentials, and cross-sector training fellowships, ultimately positioning the empowered, observant production worker as the most critical and effective security control in the age of AI-mediated threats.

Acknowledgement

This paper is dedicated to Eliana Friedman, whose love, joy, and teaching will be missed by all of the communities she worked so hard to reach.

Ethics Declaration: This paper is a conceptual and policy-oriented study that uses anonymized stakeholder material supplied for illustrative purposes.

AI Declaration: AI tools within Google Docs, ChatGPT, and Claude were used to assist with drafting, restructuring, formatting and reference checking under author direction. The author remains responsible for the argument, source verification, final wording and all claims submitted for publication.

References

Acharya, D.B., Kuppan, K. and Divya, B. (2025) 'Agentic AI: Autonomous intelligence for complex goals—A comprehensive survey', IEEE Access, 13, pp. 18912–18936. doi: 10.1109/ACCESS.2025.3532853.

Adeoye, S.O., Lindberg, H., Bagby, B., Brown, A.M., Batarseh, F.A. and Kaufman, E.K. (2023) 'Cyberbiosecurity workforce preparation: Education at the convergence of cybersecurity and biosecurity', NACTA Journal, 67(1), pp. 341–351. doi: 10.56103/nactaj.v67i1.151.

Administration for Cyber Security (2026) 'Foreign hackers launch AI Agent attacks against government agencies; Ministry of Digital Affairs activates coordinated response and strengthens cybersecurity defenses', Ministry of Digital Affairs, Taiwan, 13 August. Available at: https://moda.gov.tw/ACS/press/news/press/20394

Barnett, M., Womack, J., Brito, C.E., Miller, K., Potter, L. and Palmer, X.-L. (2024) 'Botnets in healthcare: Threats, vulnerabilities, and mitigation strategies', European Conference on Cyber Warfare and Security, 23(1), pp. 58–65. doi: 10.34190/eccws.23.1.2345.

Bokulich, N.A. and Bamforth, C.W. (2013) "The microbiology of malting and brewing", Microbiology and Molecular Biology Reviews, Vol 77, No. 2, pp 157-172, doi:10.1128/MMBR.00060-12.

Das, P., Chakraborty, S., Narula, S., Potter, L., Palmer, X.-L., Rana, P., Takabi, D. and Ghasemigol, M. (2026) 'BioShield: A context-aware firewall for securing Bio-LLMs', arXiv, arXiv:2603.22612. doi: 10.48550/arXiv.2603.22612.

Dream Research Labs (2026) 'Inside a multi-agent AI framework used to compromise government entities in Asia', Dream Security Blog, 12 August. Available at: https://www.dreamgroup.com/blog/inside-a-multi-agent-ai-framework-used-to-compromise-government-entities-in-asia

Duncan, S.E., Reinhard, R.G., Williams, R.C., Ramsey, F., Thomason, W., Lee, K., Dudek, N., Mostaghimi, S., Colbert, E. and Murch, R.S. (2019) "Cyberbiosecurity: A new perspective on protecting U.S. food and agricultural system", Federal Institute for Vocational Education and Training (BIBB) (2026) 'The dual system: Young people study in the company and at school'. Bonn: Bundesinstitut für Berufsbildung. Available at: https://www.bibb.de/en/77203.php

Federal Ministry for Economic Affairs and Energy (BMWi) (2021) Verordnung über die Berufsausbildung zum Brauer und Mälzer und zur Brauerin und Mälzerin (Brauer- und Mälzerausbildungsverordnung – BrauMäAusbV), 4 June 2021, BGBl. I, p. 1483. Available at: https://www.gesetze-im-internet.de/braum_ausbv/ (Accessed: 24 August 2026).

Frontiers in Bioengineering and Biotechnology, Vol 7, Article 63, doi:10.3389/fbioe.2019.00063.

European Parliament and Council. (2022) "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union", Official Journal of the European Union.

Firoozjaei, M.D., Mahmoudyar, N., Baseri, Y. and Ghorbani, A.A. (2022) 'An evaluation framework for industrial control system cyber incidents', International Journal of Critical Infrastructure Protection, 36, 100487. doi: 10.1016/j.ijcip.2021.100487

Gomez-Corona, C., Escalona-Buendia, H.B., Garcia, M., Chollet, S. and Valentin, D. (2016) "Craft vs. industrial: Habits, attitudes and motivations towards beer consumption in Mexico", Appetite, Vol 96, pp 358-367, doi:10.1016/j.appet.2015.10.002.

Hattoh, G., Ayensu, J., Ofori, N.P., Eshun, S. and Akogo, D. (2025) "Can large language models design biological weapons? Evaluating Moremi Bio", arXiv, arXiv:2505.17154, doi:10.48550/arXiv.2505.17154.

International Electrotechnical Commission (IEC) (2024) IEC 62443-2-1:2024 Security for industrial automation and control systems—Part 2-1: Security program requirements for IACS asset owners. Geneva: International Electrotechnical Commission.

Kirin Holdings Company, Limited (2025) 'Global beer consumption by country in 2024', 22 December. Available at: https://www.kirinholdings.com/en/newsroom/release/2025/1222_01.html

Kumar, R., Kela, R., Singh, S. and Trujillo-Rasua, R. (2022) 'APT attacks on industrial control systems: A tale of three incidents', International Journal of Critical Infrastructure Protection, 37, 100521. doi: 10.1016/j.ijcip.2022.100521.

Langner, R. (2011) 'Stuxnet: Dissecting a cyberwarfare weapon', IEEE Security & Privacy, 9(3), pp. 49–51. doi: 10.1109/MSP.2011.67.

Manning, L. and Kowalska, A. (2026) 'The threat of ransomware in the food supply chain: A challenge for food defence', Trends in Organized Crime, 29, pp. 77–105. doi: 10.1007/s12117-023-09516-y.

Meier-Dornberg, T., Kory, O.I., Jacob, F., Michel, M. and Hutzler, M. (2018) "Saccharomyces cerevisiae variety diastaticus friend or foe? Spoilage potential and brewing ability of different Saccharomyces cerevisiae variety diastaticus yeast isolates by genetic, phenotypic and physiological characterization", FEMS Yeast Research, Vol 18, No. 4, foy023, doi:10.1093/femsyr/foy023.

Mouton, C.A., Lucas, C. and Guest, E. (2023) The Operational Risks of AI in Large-Scale Biological Attacks, RAND Corporation, Santa Monica, doi:10.7249/RRA2977-1.

Mouton, C.A., Lucas, C. and Guest, E. (2024) The Operational Risks of AI in Large-Scale Biological Attacks: Results of a Red-Team Study. Santa Monica, CA: RAND Corporation. Report RR-A2977-2.

Murch, R.S., So, W.K., Buchholz, W.G., Raman, S. and Peccoud, J. (2018) "Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy", Frontiers in Bioengineering and Biotechnology, Vol 6, Article 39, doi:10.3389/fbioe.2018.00039.

National Institute of Standards and Technology. (2020) Workforce Framework for Cybersecurity (NICE Framework), NIST Special Publication 800-181 Revision 1, NIST, Gaithersburg, doi:10.6028/NIST.SP.800-181r1.

National Institute of Standards and Technology. (2023) Guide to Operational Technology (OT) Security, NIST Special Publication 800-82 Revision 3, NIST, Gaithersburg, doi:10.6028/NIST.SP.800-82r3.

Palmer, X.-L., Potter, L., Lesaja, S., Karathanasis, S. and Ghasemigol, M. (2026) 'Biosecure-LLM framework: Protecting LLMs from cyberbiosecurity threats and the case for independent AI safety governance', in Clark, U., Pence, T. and Karabacak, B. (eds.) Proceedings of the 21st International Conference on Cyber Warfare and Security (ICCWS 2026). Academic Conferences and Publishing International Limited, pp. 743–750. doi: 10.34190/iccws.21.1.4524.

Potter, L. and Palmer, X.-L. (2021) 'Human factors in biocybersecurity wargames', in Arai, K. (ed.) Advances in Information and Communication: Proceedings of the 2021 Future of Information and Communication Conference (FICC), Volume 1. Cham: Springer, pp. 666–673. doi: 10.1007/978-3-030-73100-7_48.

Potter, L. and Palmer, X.-L. (2023) "Mission-aware differences in cyberbiosecurity and biocybersecurity policies: Prevention, detection, and elimination", in Greenbaum, D. (ed.) Cyberbiosecurity. Cham: Springer, pp. 37–69, doi:10.1007/978-3-031-26034-6_4.

Raihofer, L., Zarnow, M., Gastl, M. and Hutzler, M. (2022) 'A short history of beer brewing: Alcoholic fermentation and yeast technology over time', EMBO Reports, 23(12), e56355. doi: 10.15252/embr.202256355.

Richardson, L.C., Connell, N.D., Lewis, S.M., Pauwels, E. and Murch, R.S. (2019) "Cyberbiosecurity: A call for cooperation in a new threat landscape", Frontiers in Bioengineering and Biotechnology, Vol 7, Article 99, doi:10.3389/fbioe.2019.00099.

Soice, E.H., Rocha, R., Cordova, K., Specter, M. and Esvelt, K.M. (2023) "Can large language models democratize access to dual-use biotechnology?", arXiv, doi:10.48550/arXiv.2306.03809.

Török, T.J., Tauxe, R.V., Wise, R.P., Livengood, J.R., Sokolow, R., Mauvais, S., Birkness, K.A., Skeels, M.R., Horan, J.M. and Foster, L.R. (1997) 'A large community outbreak of salmonellosis caused by intentional contamination of restaurant salad bars', JAMA, 278(5), pp. 389–395. doi: 10.1001/jama.1997.03550050051033.

U.S. Department of Education (2026) 'Perkins V'. Washington, DC: U.S. Department of Education, Office of Career, Technical, and Adult Education. Available at: https://www.ed.gov/adult-programs/adult-education-laws-and-policy/perkins-v

Xu, H., Wang, S., Li, N., Wang, K., Zhao, Y., Chen, K., Yu, T., Liu, Y. and Wang, H. (2024a) "Large language models for cyber security: A systematic literature review", arXiv, doi:10.48550/arXiv.2405.04760.

Xu, J., Stokes, J.W., McDonald, G., Bai, X., Marshall, D., Wang, S., Swaminathan, A. and Li, Z. (2024b) "AutoAttacker: A large language model guided system to implement automatic cyber-attacks", arXiv, doi:10.48550/arXiv.2403.01038.

Zhong, V., Ketchum, N., Mackenzie, J.K., Garcia, X. and Rowley, P.A. (2024) "Inhibition of diastatic yeasts by Saccharomyces killer toxins to prevent hyperattenuation during brewing", Applied and Environmental Microbiology, Vol 90, No. 10, doi:10.1128/aem.01072-24.