Teaching Ethical Hacking for the Bioeconomy: A Cyberbiosecurity Curriculum in Practice

CFP Submission for CyberBio 2026

Charles Frick, Johns Hopkins Applied Physics Laboratory

Session Overview

This presentation describes a hands-on cyberbiosecurity curriculum developed to introduce high school students to the security challenges of modern biotechnology environments. As the bioeconomy increasingly relies on connected laboratory systems, cloud-based research platforms, and automated biological workflows, there is a growing gap between workforce needs and available educational pathways. This effort addresses that gap by providing early, practical exposure to cyberbiosecurity concepts through realistic scenarios, ethical hacking exercises, and defensive remediation activities.

The curriculum is delivered as an immersive, one-day workshop that combines foundational instruction with guided technical labs executed in isolated virtual environments. Rather than focusing on abstract cybersecurity theory or biology concepts in isolation, the workshop emphasizes how cyber vulnerabilities directly affect biological data, laboratory operations, and research integrity. The presentation draws on multiple years of curriculum delivery and refinement, highlighting lessons learned from deploying the program at scale and collaborating with bioeconomy stakeholders.

Curriculum Design Approach

The curriculum was intentionally designed to be:

- Accessible to students with no prior cybersecurity or biology background
- Safe to execute without risk to real systems or data
- Grounded in realistic biotechnology use cases
- Explicitly framed around ethics, legality, and responsible defense

Each student accesses a self-contained virtual lab environment through a web browser, eliminating local installation requirements and enabling consistent delivery across diverse classroom settings. Environments include a simulated biotechnology system containing representative biological data artifacts, allowing students to observe how common software vulnerabilities can lead to credential theft, data exfiltration, or system misuse.

Instruction follows a structured progression:

1. Introduction to the bioeconomy and cyberbiosecurity risk
2. Legal and ethical foundations of vulnerability research
3. Guided discovery and exploitation of known vulnerabilities
4. Analysis of downstream impacts on biological data and operations
5. Defensive remediation and discussion of detection strategies

This approach ensures that exploitation techniques are always contextualized as a means to understand and prevent harm, not as an end in themselves.

All curriculum materials are distributed under Creative Commons licenses, enabling educators and organizations to adopt, adapt, and scale the program without cost barriers. This open distribution model supports broader workforce development goals across the bioeconomy.

Audience Takeaways

Attendees will leave with:

- A concrete example of an operational cyberbiosecurity education model
- Practical insight into safely teaching adversarial concepts in biological contexts
- Lessons learned from deploying hands-on cyberbiosecurity training at the secondary education level
- A replicable approach for building early workforce capacity in the bioeconomy

This session is particularly relevant for educators, workforce development leaders, policymakers, and practitioners interested in strengthening the cyberbiosecurity talent pipeline through applied, ethics-driven education.