Bryan Gregg

CYSE_200T (202520_SPRING_CYSE200T_28058)

CRISPR Gene Editing and DNA Cybersecurity Risks

Task A - Data & Privacy Risks to DNA Analysis systems

Risks:

> Malicious code compromising DNA sequences - Since DNA and digital information are being combined there is a risk that it can become compromised and then used against the DNA analysis system to access and essentially hack into other DNA sequences within the system. According to the text this could possibly affect health care systems that use DNA analysis as well as institutions that are researching certain DNA sequences that also use an analysis system for example.

Mitigation:

After reading the text I believe that a good way to mitigate some of the damage that can be done by malicious code that has compromised DNA sequences is to have a secure sequencing pipeline for example. Like one of the other students explained in the comments, it can be an encrypted sequence of data taken as a sample and can be used when authenticating the data sequence in the analysis system. This way it can safeguard against malicious code trying to access the system to cause harm. I thought that was a very good example to use as a mitigation technique.

Task B – Ethical Considerations Over CRISPR

Some of the ethical considerations around CRISPR gene editing are mainly centered on its safety, who has access to it, and what society thinks about it. Obviously, safety would be #1 as there is no long-term study showing the effects of how gene editing can affect humans. So far as social impact goes, that can vary depending on who you ask, what somebody's beliefs are, or the culture that this technology is being used in. Finally, who has access to this technology is extremely important. You do not want it to fall into the wrong hands, and you certainly do not want it to be exclusive to it

a select few. There are a lot of variables that go into this when deciding whether it should be acceptable to be used at all.