'Cyberbiosecurity' and protecting the life sciences

December 7 2017

Biology and biotechnology have entered a digital age, but security policies around such activities have not kept pace.

That's according to Colorado State University's Jean Peccoud, Abell Chair of Synthetic Biology and professor in the Department of Chemical and Biological Engineering. Peccoud is lead author on a new paper in *Trends in Biotechnology*, published online Dec. 7, urging awareness of "cyberbiosecurity" risks for researchers, government and industry.

Co-authored by CSU postdoctoral fellow Jenna Gallegos and colleagues at the University of Nebraska and Virginia Tech, the paper outlines how the evolving nature of biotechnology should sound alarm bells for new ways to keep life sciences assets safe. This could be from accidental cyber-physical breaches, or more nefarious threats.

"In the past, most biosecurity and biosafety policies were based on sample containment," Peccoud says. "Now, it's so easy to read DNA sequences, for example, or to make DNA molecules out of sequences publicly available from bioinformatics databases. Most projects have a cyber dimension, and that introduces a new category of risk."

Peccoud is a synthetic and computational biology who specializes in the design of new DNA molecules. He has led trainings for federal government agencies interested in increasing security around life sciences infrastructure, and has also helped assess the state of the nation's biodefense infrastructure.

Peccoud and co-authors explain that security policies in the life sciences fall into two categories: biosafety and biosecurity. Biosafety procedures are designed to prevent exposure to pathogens and accidental release of biological agents. Such measures include protective clothing, sterilization procedures and airlocks.

Biosecurity policies, however, are usually associated with travel, supply chains, or terrorist activities. Breaches of biosecurity can be accidental (a traveler bringing contaminated material from overseas) or intentional (bioterrorism).

Such policies fall short in protecting against threats from "the intricate relationship between computational and experimental workflows," according to the paper.

Nowadays, software tools can design DNA sequences with new properties. Gene synthesis techniques can theoretically be used to develop biological weapons derived from genomic sequences of pathogens. In fact, the federal government has developed new screening guidelines for providers of gene synthesis services.

Peccoud stresses that cyberbiosecurity risks are not always doomsday scenarios. There's a broad spectrum of risks that can start with fairly low-impact mistakes, such as mislabeled samples in a lab. Despite the risks, there is too much naive trust among partners in the biotechnology supply chain. That needs to change, he says, in order to increase productivity around biological research and to limit the risk of a significant incident.

Peccoud likens this needed change to today's increasing awareness around cybersecurity, in response to high-profile hacking incidents of credit card and other companies. Decades ago, it was possible to use computer systems without a password, and it was common for several employees of a company to share a computer. Today, most people have

at least some sense of how to manage their own cybersecurity. The same should be true for the life sciences, he says, and a major incident shouldn't need to be the impetus for change.

The authors recommend employee training, systematic analyses to examine potential exposure to cyberbiosecurity risks, and the development of new policies for preventing and detecting security incidents.

"Once individuals in a community are aware of cyberbiosecurity risks, they can begin to implement safeguards within their own work environments, and work with regulators to develop policies to prevent cyberbiosecurity breaches," they write.

More information: *Trends in Biotechnology* (2017). www.cell.com/trends/biotechnol … 0167-7799(17)30276-7 , DOI: 10.1016/j.tibtech.2017.10.012

Provided by Colorado State University