The global covid-19 pandemic has stressed the urgency –now more than ever– for a collaboration of the Health and Technology sectors. In view of the increasing use of technology in the fields of Biotechnology and Pharmaceutical Research, new challenges arise in terms of cyber security. Although Biosecurity and Biosafety focus on physical protection from pathogens' exposure or on acts preventing terrorist activities, it seems that none of the aforementioned addresses the computational – digital threats lurking in modern research. (Peccoud et al., 2018)

Despite the undeniable cyber-attacks' impact on almost every industry worldwide, it seems that the Biotechnology's readiness level is still in its infancy, even though a significant number of attacks have already occurred (Mueller, 2020). Additional threats have to be taken into account, given the inherently sensitive data at stake. Simply put, the leaking of a credit card's data bears trivial consequences compared to the potential disruption of a virus' research or the potential intellectual damage caused by a cyber-attack in this industry.

According to a recent survey, Biotech companies perceive unauthorized access and secret data alteration as the most significant threats. They also recognize the necessity of implementing several/crucial steps to enhance defence and awareness against cyber threats. (Millett et al., 2019)

In consideration of Cybercrime's complexity and the interoperability that Health Sciences demand, it seems that Biotechnology and Pharmaceutical companies need to redefine Cyber Security's importance. It is common ground that prevention mitigates any consequences and is also crucial in financial terms. A case in point would be the aftermath of Merck's incident (Voreacos et al., 2019), which caused havoc, as compared to the efficient reaction of LabCorp that overcame the attack in a short time, avoiding further losses (Goedert, 2018).

References

Goedert, J. (2018) 'LabCorp still recovering from weekend ransomware attack', Healthdatamanagement.com, p. 1. Available at: http://0-search.ebscohost.com.serlib0.essex.ac.uk/login.aspx?direct=true&db=bsu&AN=130843337&site=eds-live (Accessed: 26 January 2021).

Millett, K., Dos Santos, E. and Millett, P. D. (2019) 'Cyber-Biosecurity Risk Perceptions in the Biotech Sector', Frontiers in bioengineering and biotechnology, 7, p. 136. doi: 10.3389/fbioe.2019.00136.

Mueller, S. (2020) 'Facing the 2020 Pandemic: What does Cyberbiosecurity want us to know to safeguard the future?', Biosafety and health. doi: 10.1016/j.bsheal.2020.09.007.

Peccoud, J., Gallegos, J., Murch, R., Buchholz, W., Raman, S. (2018) 'Cyberbiosecurity: From Naive Trust to Risk Awareness', Trends in biotechnology, 36(1), pp. 4–7. doi: 10.1016/j.tibtech.2017.10.012.

Voreacos, D., Chiglinsky, K. and Griffin, R. (2019) 'Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?', Bloomberg.com, p. N.PAG. Available at: http://0-search.ebscohost.com.serlib0.essex.ac.uk/login.aspx?direct=true&db=bsu&AN=140068257&site=eds-live (Accessed: 27 January 2021).