This discussion intended to examine Cyber Security's impact on Biotechnology-Pharmaceutical and the Health Sciences' sector as a whole.

It is common ground that Cyber-attacks are exponentially increasing in every business sector, costing billions in terms of damages. Known rogue techniques as phishing, Denial of Service, and ransomware are performed on a minute basis, aiming to extort money, information, intellectual assets, or as a means of sabotage.

Examined in the global covid-19 pandemic context, health sciences currently hold the most prominent place in our everyday life, as the world is hoping for science research to win the virus challenge. Simultaneously, the interoperability and the digitization of modern research, coupled with the limited personnel's security skillset and awareness led to the increase of breach incidents.

According to a survey, the Biotechnology sector's most significant threats seem to be unauthorized access and data alteration, leading to research's mistrust and disruption (Millett et al., 2019). Although this may be true, in some extreme cases, the consequences of a cyber-attack in the Health Industry could also result in human demise (Chawla, 2021). In the same fashion, Cyber-perpetrators have also targeted the covid-19 vaccine distribution supply chain, upgrading cyber-crime to an entirely different level (Murerwa, 2021).

In the final analysis, it was commonly agreed that Cyber Security nowadays is not an option but a vital necessity for business continuity and human prosperity. Organizations worldwide have already made some changes due to the GDPR; nonetheless, that is merely a small step (Wilson, 2021).

More endeavours in terms of budget and human resources are required. Risk assessments and Cyber Security best practices should be an ongoing process in every industry. Additionally, present-day software and applications must be aligned with secure coding principles to mitigate potential vulnerabilities, especially since new technologies add value to these efforts (i.e., A.I & Machine Learning).

**References**

Chawla, V. (2021) Initial Post – Cyber Security's impact on Health Sciences. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=240220 [Accessed 2 February 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.

Murerwa, R. (2021) Initial Post – Cyber Security's impact on Health Sciences. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=240220 [Accessed 4 February 2021]

Navaratnasingam, A. (2021) Initial Post – Cyber Security's impact on Health Sciences Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=240220 [Accessed 2 February 2021]

Wilson, C. (2021) Initial Post – Cyber Security's impact on Health Sciences. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=240220 [Accessed 2 February 2021]