From my group research I realized the healthcare industry has become the prime target for cyber criminals due to its vulnerability and ease of infiltration. While technology continues to advance and so does healthcare systems, the cybersecurity departments on the other hand are struggling to keep up to date leaving patient information at risk in the event of an attack. Most healthcare organizations today do not have many competent cybersecurity staff with the necessary expertise or proper incident response plans to respond to when being under attack because the position takes longer to fill in than anything else. The attacks can be from DDoS, Phishing emails, Ransomware, Data Breaches to Hacking into Staff Accounts. These data hold private details of a patient that can be sold for money on the black market. This is a serious issue for the industry as many healthcare organizations lose their reputation and significant resources because of it.

To address these issues, ethical implementation strategies can be implemented such as strong encryption and data protection to secure sensitive patient information, this keeps the data protected from any intruders. And by viewing cybersecurity as an ethical imperative, healthcare organizations can protect patient well-being, build trust, and ensure the integrity of the healthcare system. Training for staff members on a regular basis on security part can also significantly reduce the risk of falling victim to attacks. Another essential aspect is building an incident response plan, organizations must have a solid and tested plan in place in the event of an attack to reduce the damages and recover from the breach fast. To ensure preparedness, this includes creating clear channels of communication, designating incident response teams, and running frequent drills and testing. The organizations should Invest more resources to strengthen security measures as this will prove to be beneficial in the long run, since it toughens the security and makes it harder for attackers to get in.

However, there are a few possible negatives outcomes to be considered such as the cost of using ethical implementation strategies is one difficulty itself. Another is finding competent cybersecurity staff in the field. Because there is a much greater demand than supply for trained cybersecurity staff, it is challenging for healthcare organizations to find and keep experienced personnel. The development and maintenance of efficient ethical security measures may be affected by this lack of expertise. Additionally, it can result in higher expenses for hiring or contracting out security operations to other organizations. Furthermore, applying ethical implementation strategies can be difficult due to their complexity. To manage encryption procedures, incident response strategies, and other cybersecurity measures successfully, healthcare organizations may need to have specialized knowledge and technological skills to do so. Without the right knowledge and instructions, there is a chance of errors which can leave the system vulnerable for the attackers to breach into.

In conclusion, the healthcare industry must address its vulnerability to cybercrime through ethical implementation strategies. By employing strong encryption, creating incident response plans, and investing in staff training and resources, healthcare organizations can prevent the risks from being targeted, protecting patients' information, and maintain the trust of both patients and the wider healthcare community.