Collaborative Discussion 1 – Received Response – Muhammad Qasim

Thank you for the discussion. A good job done on the topic and issues. The post is insightful and well-detailed on the issues discussed in Compromising a Medical Mannequin. The study was in the paper was a project conducted to investigate vulnerabilities in the IT sector of health care. The quote in the first paragraph tells us that technology in healthcare is evolving and becoming more prevalent but a big drawback is how security is lacking. The definitions of brute force attack and DOS attacks were well discussed and illustrations are given on how the events were carried out in the project. The BackTrack5 program carried the brute force attack that was successful. A DoS attack was also carried out. Any healthcare provider that utilizes a computer network holds, transacts, processes and stores information or contracts with a vendor to do so on their behalf is at risk for security exposure. The post vividly discussed ways of preventing these attacks. Looking at events such as the Aetna data breach makes one thing clear: every organization needs to be aware of risks like these, as well as devote additional attention toward mitigating IT risks and working with an agent who is an expert in healthcare compliance matters. Patient information related to health in the form of reports, personal data, prescriptions are confidential and the medical industry needs to maintain its integrity in maintaining the confidentiality and misuse of available information and thus it is important to know the vulnerabilities of such systems (Ronquillo et al. 2018). From the discussion, One can clearly understand these vulnerabilities.

References:

McLeod, A. and Dolezel, D., 2018. Cyber-analytics: Modeling factors associated with healthcare data breaches. Decision Support Systems, 108, pp.57-68.