Jason Loo

Engr 30

RW 3: Medical Implant Risk Analysis

To give a brief summary of the article, this company Corazon, created an implantable heart monitoring system that monitors heart activity and shares any information with medical providers. A device like this is ahead of its time and received many approvals and were also able to provide such device to lower income individuals

The problem came when a researcher was able to find a breach in the wireless connectivity of the device and mentioned it to the company, however Corazon found the risk of harm to be negligible. In a situation such as this, it should come down to the consumer and consent should be approved by the users, not the company. The company failed to relay this information to the consumers and make sure that they made a completely rational decision when evaluating this information. A majority of the users would have probably wanted a patch to be released and the company should then honor that request.

Corazon failed to notify any part of the public about this risk, and because they were not transparent, the public was not aware of any of these breaches. If the breach was exploited while the company knows about this, I am sure they would lose the trust of the public and eventually go under and disappear as a company. All this is doing is merely covering liability.

One way Corazon could have identified these errors is though using a fault tree analysis. Here we start out with an undesirable event, then we branch out to look for hazards. So in the case of this event, we would start out with this breach of security, then work our way through what kind of information may be exposed, birthdays, passwords, medical information, etc. Then from there, assuming hackers have the worst intentions, they may use this information to sell to other individuals or may try to access other accounts. Birthdays tend to be many individual’s passwords so it would cause a much bigger problem than it needs to be.