

Nicholas Garrett

Professor Dailmari

Math 3316

9/14/2021

Assignment 2

- **intro**

Corazón, according to the case study, is a startup company that builds an implantable medical device for monitoring heart health.

This monitoring device has a phone app so the data collected by the device can be used by patients and medical providers alike. This data is transmitted to the phone via a short range communication system with all data being encrypted.

However, at a recent conference on security, a researcher claimed the existence of, and presented a proof-of-concept demonstration, of a flaw that would allow another party, other than the patient or medical provider, to interfere with the commands being passed to the Corazón device.

In response to this presentation, the technical leaders as well as a researcher at Corazón determined the risk posed by this attack to be minimal.

- **body**

The CARE system outlines a way to consider this case from an analytical standpoint. The steps for CARE are Consider, Analyze, Review, and Evaluate.

- **Consider stakeholders and consequences**

Following the first step in the CARE process, we shall consider who the stakeholders are in this situation. Who are they? What effects will the actions decided on have on these groups or individuals?

The stakeholders and actors respectively are the customers of Corazón, as it is their purchased heart-monitoring device that could be insecure, and the technical leaders and researcher of Corazón, as it was their decision whether or not to consider the security vulnerability as a viable threat, with the researcher having discovered this threat to security joining them in this category.

For the customers, an effect this vulnerability could have, as stated previously, is that it is their purchased product that could be made to malfunction or cease to operate entirely. As it is an implantable system, by an attacker gaining access to the device, further probing for vulnerabilities could occur. In this instance, the attack may only be able to reset the device. However, it proves that it is possible to remotely control the system without authorization. Who knows what possibilities for attack this could unlock in the future?

- **Analyze how the code applies in this context**

asda

- Review possible outcomes

sdf

- Evaluate decisions and future impact

asdf

- conclusion

asdfs

- references

asdfa