HIPSTER Project

Helping developers in innovative Health IoT companies make decisions about Security, Privacy, and Safeguarding

Charles Weir, Anna Dyson, Dan Prince
Security Lancaster

Introduction

Health IoT innovation offers vast potential benefits, providing both health monitoring and intelligent interventions. But there are huge potential Cyber Security, Privacy and Safeguarding (SPS) dangers with the resulting devices and systems. The teams producing the innovation tend to be in small companies and often lack professional security expertise. Scarce money and effort may be spent addressing the wrong problems.

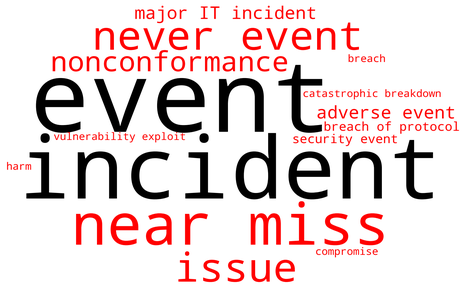
Objective

In the Hipster Project, we are creating an intervention, incorporating professional and community evidence, to help teams make those Health IoT SPS decisions in a more cost effective and efficient way.

In Health IoT security, ‘threat actors’ are often the heroes…not the villains!

Method

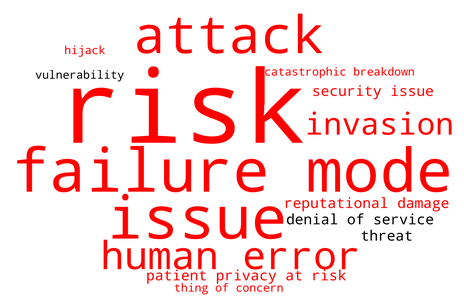
After our initial interview survey of stakeholders, we shall iterate, using Design Based Research to create and trial both (1) a suitable workshop intervention, and (2) a theory around how and why this intervention works.



Results/Findings

Our initial survey highlighted:

- Often the threat actors are heroes (medical staff), not villains.
- There are many dialects of cybersecurity, even within a single domain.
- Most participants considered security aspects both as ‘entry stakes’ and as sales points.



This work was supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC under grant number EP/S035362/1