Cyber by Sighbear Threats

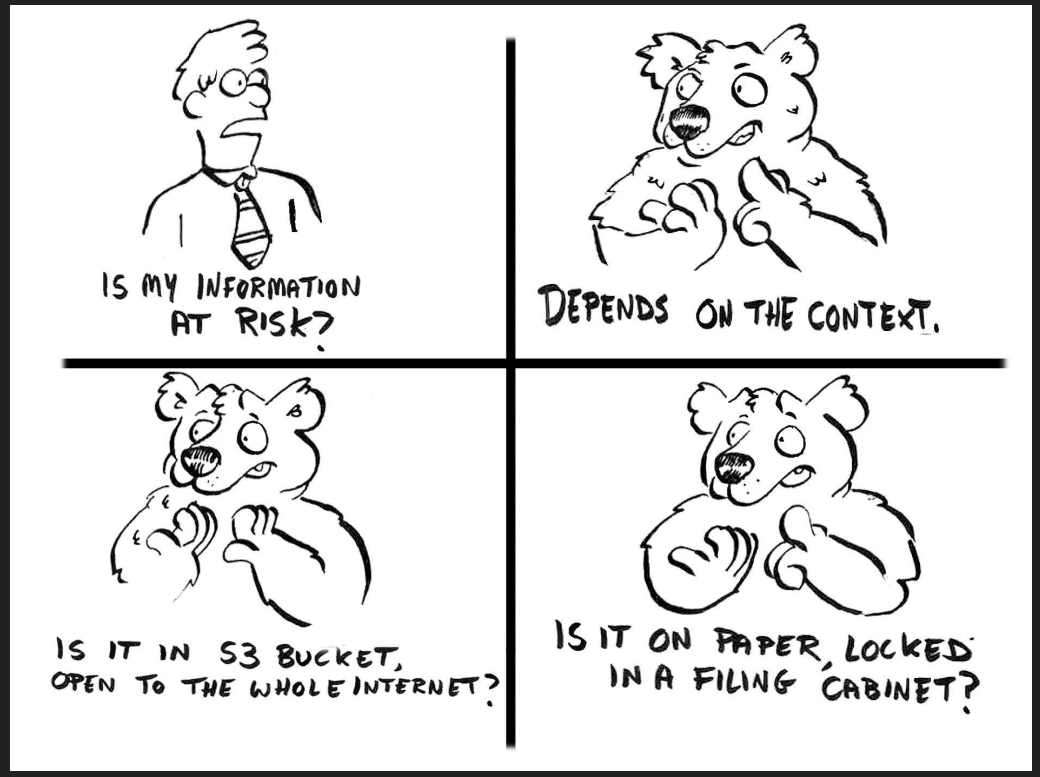
What risk are the CiBears at without threat?

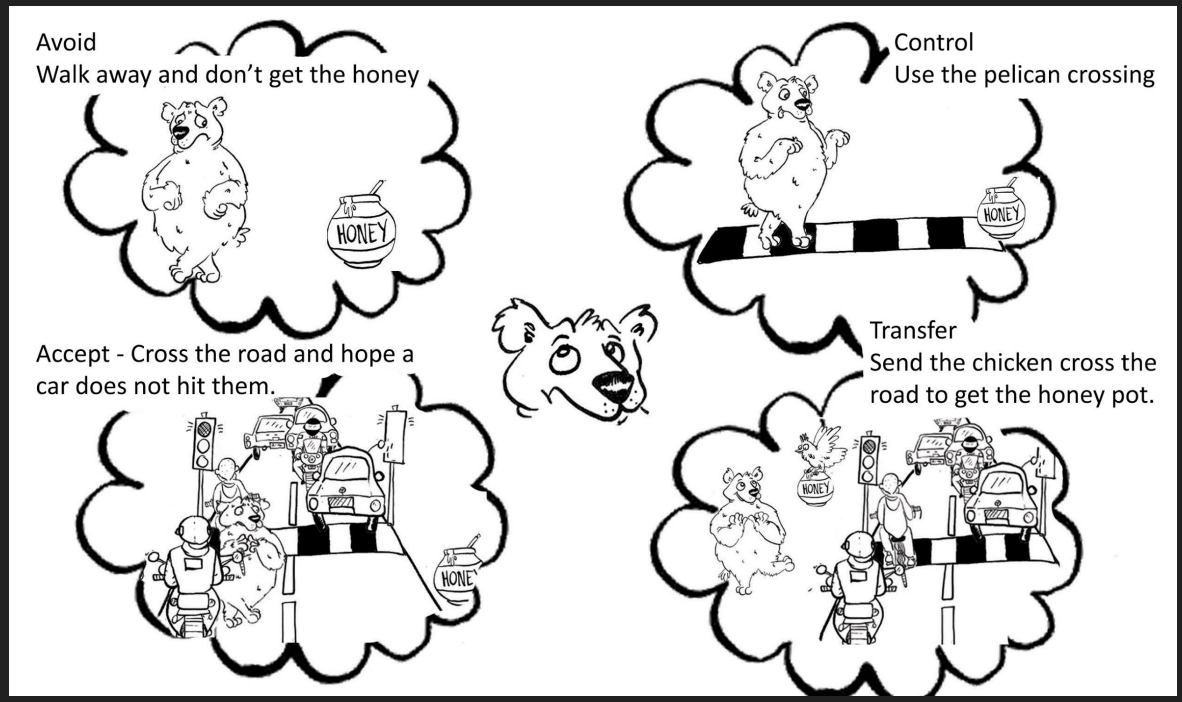
v1.0

Previously on SighBearUK Education

- If you have not seen part 1 or part 2 or need a detailed refresher see https://www.sighbear.uk/Cyber-Education/

- In the first slide deck we covered Cyber & Risk.





- In the second deck we cover CONTEXT

The story today!

Threat - Introduce it

What is threat?

- Definition of threat
  - “a statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not done.”

Threat - questions to think about

- Threat (questions to ask yourself as the asset owner)
  - Who would want to attack your assets
  - Why would they want to (what is their motivation)
  - How skilled are they (what is their capability, script kiddies or state sponsored)
  - What is most important to the attacker (disclosure, integrity, availability)
  - how would they go about the attack, technical or social, pay an insider, etc
- This gives you an idea of likelihood for the risk equation

Threat as in input into likelihood

Note: This is a follow on / expansion of the likelihood slide in Slide Deck One @ https://www.sighbear.uk/Cyber-Education/

- Likelihood is made up of two parts
- Motivation
  - having a reason to do something
- Capability
  - Having the skills, tools, etc

Motivation

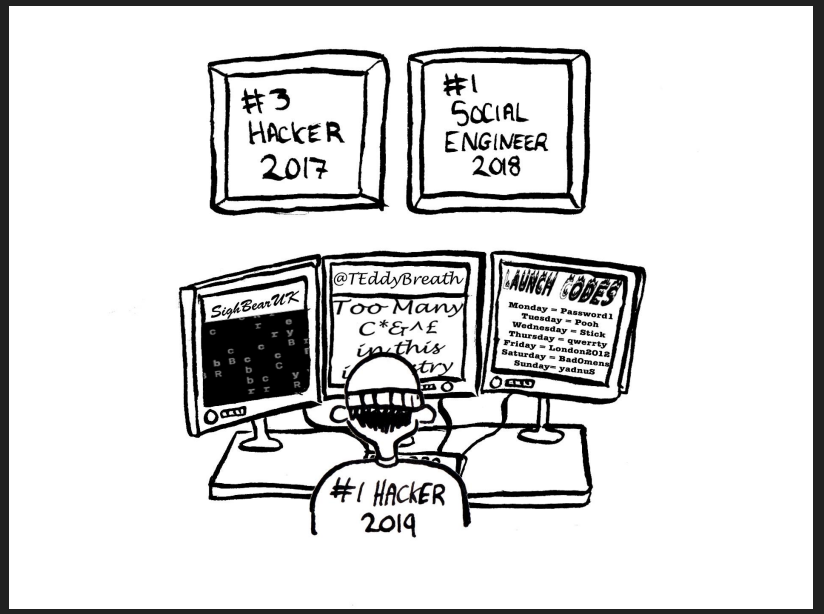
- Definition
  - “a reason or reasons for acting or behaving in a particular way.”

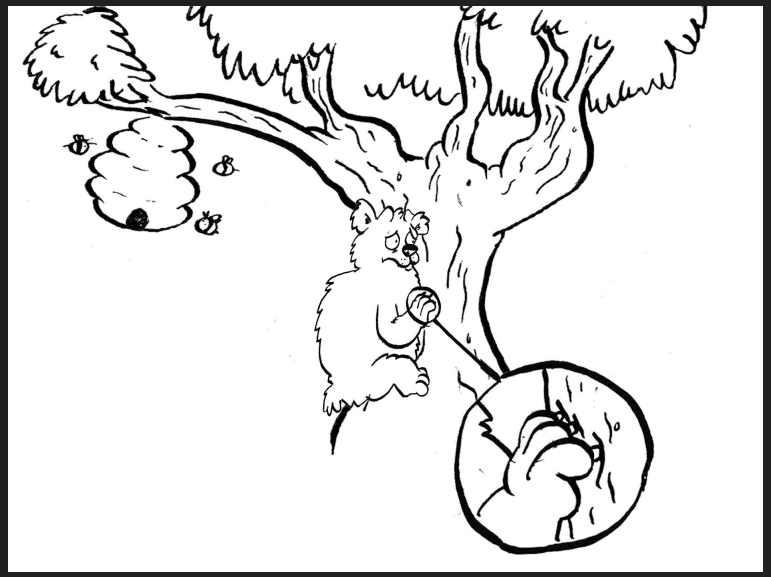
- Cyber Motivation
  - Cyber Criminal wants to steal money, activist to embarrass a government through website defacement, etc

- Sighbear Motivation
  - to get some honey to provide energy to catch some salmon

Capability

- Definition of capability
  - “the power or ability to do something.”
- Cyber Capability
  - Having the skills (not just technical but can be social as well), tools, finances, etc
- Sighbear Capability
  - Skills (i.e. climbing trees) tools (claws to help climbing)





Examples of possible threats

- Threat to Confidentiality (“the state of keeping or being kept secret or private.”) -
  - Cyber Criminal wants to know your login details to your bank so they can steal your money.

- Threat to Integrity (“ensuring that data/information is real, accurate and safeguarded from unauthorized user modification”)
  - Organised crime want to change prison records to get someone released early.

- Threat to Availability (“ensure that required data/information is always accessible when and where needed”)
  - Foreign government wants to take another government’s online voting service offline at key moment.

What's coming next?

Vulnerabilities expanded

Likelihood (introduce probability subjectiveness)

Art of A+D (Attack + Defence)

Threat modelling

Risk methodologies

Credits

If you have a cyber challenge, maybe you would like to hire the **CiBears** and friends**?**

Twitter @sighbearuk
web www.sighbear.uk

Artwork by Claire Brown https://clairebrown.myportfolio.com