Cyber by Sighbear Threats

What risk are the CiBears at without threat?

v1.0

Welcome to more Cyber by Sighbear in association with the CiBears.

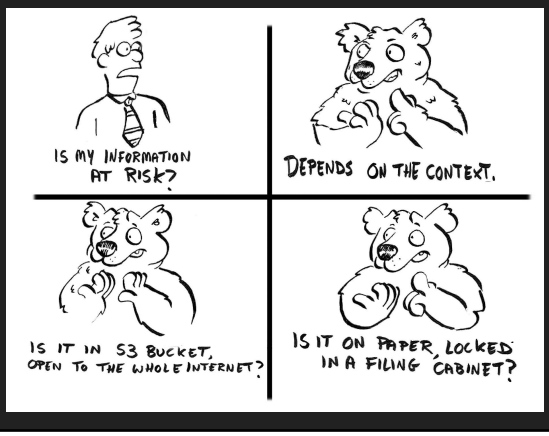
This slide deck expands on the initial story of Cybersecurity and continues the journey for those who wish to get into the industry and as a refresher to those already in the industry as to how and why we do Cyber Security.

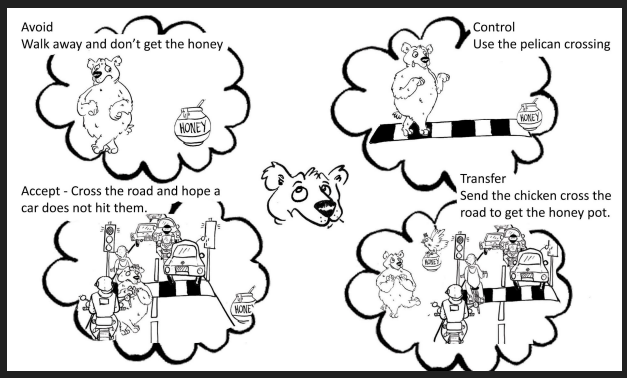
This is the third slide deck and there will be others that expand on the areas covered in this one and related areas.

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

In the first slide deck we covered Cyber & Risk and definitions for them both.

We joined Cyber and Risk together for Cyber-Risk with simple risk equation (R = V * L * I) along with risk management approaches .

- Avoid
- Control
- Accept
- Transfer

In the second deck it was all about CONTEXT (sorry for shouting but it seems to be an issue for some, understanding context)

Lady - Is four a lot
Man - Depends on the context
Man - Dollars? no
Man - Murders? yes

Credit @warmana (on twitter)

The story today!

Threat - Introduce it

As it says on the slide today we are going to cover threat.

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.”

Understand what threat is

Who wants to do harm to you, what will they use to do harm to you and how much effort are they going to expend to do that harm?

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

So as the slide states, think about who is a cyber threat.

Who are the attackers (the persons carrying out the attacks)?

Why do they want to attack you (what's their motivation), maybe rather than attack someone else instead of you?

What skills and resources (money, time, computing power, etc) do the attackers have?

What is the outcome the attacker wishes to inflict on you?

How would the attacker go about attacking you?

All these are covered in the next few slides.

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

Likelihood is mostly made up of two things / events.

In the case of our Cyber education we are going to use Motivation and Capability which will be expanded upon in the next couple of slides.

As the image shows the SighBear has ladders (capability) but already has a pot of honey (so no motivation to disturb the bees for some honey)

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

This slide covers the wider definition of motivation "a reason or reasons for acting or behaving in a particular way.", along with a couple of examples of motivation in the Cyber world and the Sighbear world.

In the Cyber world

- A Cyber Criminal wants to steal money
- An activist to embarrass a government through website defacement.

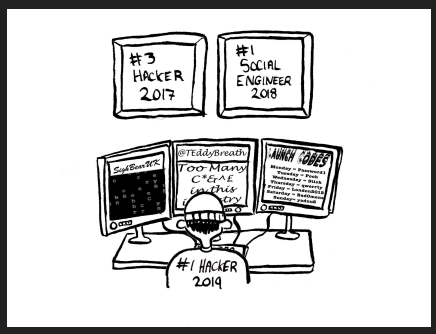
In the Sighbear world

- The bears want to some honey to provide energy to catch some salmon

These are just a few examples of what motivates people and bears.

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)



This slide covers the wider definition of capability "the power or ability to do something", along with couple of examples of capabilities in the Cyber world and the Sighbear world.

In the Cyber world

- Having the right skills (not just technical but can be social as well), tools, finances, resources etc

In the Sighbear world

- Skills (i.e. climbing trees)
- Tools (claws to help climb trees)

These are just a few examples of of what capabilities people and bears have.

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.

This slide covers threats to the security triad (watch the video link for explanation https://youtu.be/SP8cr0fg5Sg, we might expand on in future slide decks).

And how the threats might apply to Confidentiality, Integrity and Availability

What's coming next?

Vulnerabilities expanded

Likelihood (introduce probability subjectiveness)

Art of A+D (Attack + Defence)

Threat modelling

Risk methodologies

Some things that we are planning to do slide decks on.

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

Why should you consider hiring the CiBears?

Because we are like a breath of fresh air compared to some other Cyber consultants we come across because we won't:

1) Try to sell you snake oil (there is no silver bullet, or 100% security)
2) We are not security charlatans (we have a great mix of academia and real world experience)
3) We will get to know your business to ensure we give appropriate advice aligned to your needs

Mantra "Security does not say No, it says yes but ……." understand the risks.

It's a shame that @NCSC withdrew it.

User experience should be fantastic - security should be good enough

As it provided something we have believed in from before they ever published it