Cyber by Sighbear

With the CiBears talking about Cyber Risk

V1.1 (Copyleft)

Any comments / suggestion / abuse tweet @SighBearUK

Welcome to Cyber by Sighbear in association with the CiBears.

This slide deck tell the initial story of Cybersecurity 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.

The is the first slide deck and there will be others that expand on the areas covered in this one.

v1.1 update a few spelling grammar and other small things

The purpose of this slide deck and why we did it?

- We (Sighbear and the CiBears) want to help people get into Cyber.
- We also want to to do some myth busting around cyber and especially challenge the snake oil sellers and security charlatans

How to use the slide deck?

- You can just go through the slides and then look at the speak notes as you go through it again.
- Do each slide and speaker notes in the first pass and then just the slides
- Or in whatever why you like ;-))

Hopefully the slide text covers everything and does not need speakers notes

What is Cyber?

- "There are no common definitions for Cyber terms - they are understood to mean different things by different nations/organisations, despite prevalence in mainstream media and in national and international organisational statements." - NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/cyber-definitions.html
- Given this ambiguity which option will you pick for Cyber
  - From the Ancient Greek verb "to steer, to guide, to control"
  - Relating to or characteristic of the culture of computers, information technology
  - Connotes a relationship with information technology.
  - Anything relating to, or involving, computers or computer networks (such as Internet)

The main point in this slide is that there is no agreed definition of what Cyber is.

This is a wordy slide but we think it is worth reading.

It is always an interesting question to ask people "How are you defining Cyber"
and as the saying goes "No such thing as a stupid question"

What is Risk?

- A situation involving exposure to danger. (Noun)
- Expose (someone or something valued) to danger, harm, or loss. (Verb)

This slide users the Oxford English dictionary definitions of risk as both a noun and a verb.

Risk is a theme throughout this slide deck and is the foundations to decision making in the context of Cyber (and is often used elsewhere and hopefully later analogies will show)

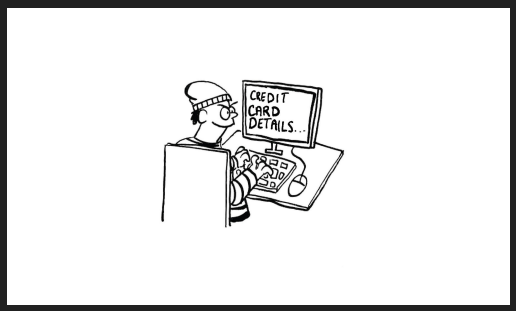
What is Cyber risk

- '**Cyber risk**' means any **risk** of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its **information technology systems**.
- There is a Cyber Risk that if you put information (i.e. credit card details) on the Internet it could be compromised

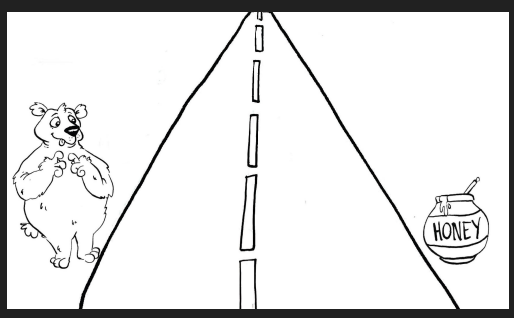
This slide brings together Cyber and Risk but since Cyber has no agreed definition for now we are going to use “Information technology systems”.

Risk scenarios

Cyber world
An online retail business does not want its customers credit card details stolen



CiBear world
The bear wants some honey for its cubs



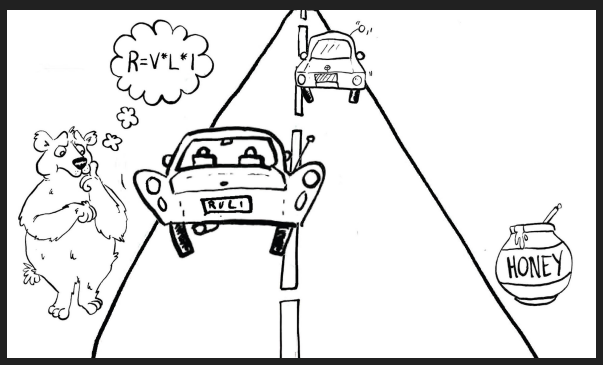
This slide describes the two scenarios.

The first is a Cyber one as the online business might go out of business if it's customers credit card details are stolen.

The second one is a more real world (rather that Cyber space) one were the bear wants some honey from across the road.

HOW DO WE UNDERSTAND RISK?

- As a simple equation like
  R = V * L * I
- As words
  "There is a risk that …… a vulnerability is likely to be exploited leading to an impact of ……."



Later slides will cover a break down of the meaning of I, V and L, but the first letter R stands for / equals Risk.

The fuller version of the wordy can be "There is a risk that …… leading to an impact of ……. which could be mitigated by ……." but mitigation is covered later in the desk.

The CiBear analogy in words "There is a risk that the CiBear might be hit by a car as he crosses the road which could lead to an impact of a serious injury"

Risk Assessment

- The a simple risk assessment using the equation
  - R = V * L * I
  - (R)isk equals (I)mpact multipled by (V)ulnerability multipled by (L)ikelihood
- Be aware there are various risk assessment methodologies, covering qualitative, quantitative, component based, system based
- The Sighbear's choice at the time of putting this slide deck together are attack trees.

So a simple way to assess risk (including Cyber risk) is through the equation R = V * L * I. We will expand on the V, L and I in the next few slides.

Quantitative Risk Analysis uses available data to produce a numerical value which is then used to predict the probability of a risk event outcome.
Qualitative Risk Analysis applies a subjective assessment of risk occurrence likelihood (probability) against the potential severity of the risk outcomes (impact) to determine the overall severity of a risk.
Component based and system based does as it says on the tin, looks at parts vs looking at the whole.

There are many method to represent the equation (to mention but a few STRIDE, MITRE, Attack Trees) but all roads lead back to RISK.

Attack trees provide a very visual representation of system based risks and is liked by the Sighbear.

Assets, Value, & (I)mpact

- An Asset – something with value to someone / business
- Value – the worth of an asset, could be money or reputation
- Impact – what is the effect if the asset is compromised
  - Confidentiality (disclosed)
  - Integrity (unauthorized change)
  - Availability {made unavailable} (denial of service)
- *Note – Impacts rarely change 'the impact is the impact' if you have £10 stolen you have it stolen even if it is in a bank in a safe with armed guards or just in your wallet you have still lost the £10*
- CiBear world - The asset is the bear and the value is its life and the impact is the bear can no longer provide food for it's cubs.

The main points are to understand what an Asset is what Value it has and what is the (I)mpact (the I from the simple equation)

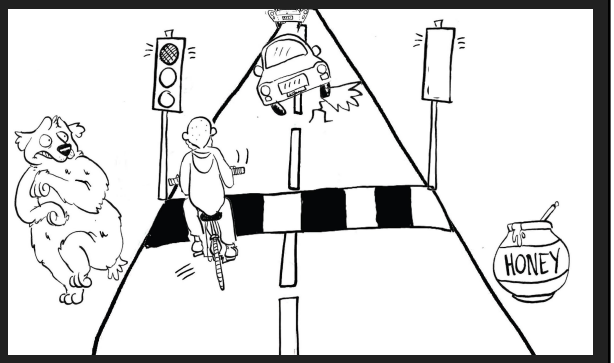
It also introduces (subtly) the "Three tenants of information security" which will be expanding in a later slide deck.

We also cover the fact the often (but not always) the impact does not change in the equation

As an example in the ongoing CiBear analogy with regards to Assets, Value and Impact.

Vulnerabilities

- Definition
  - The quality or state of being exposed to the possibility of being attacked or harmed.
- Definition (Cyber)
  - "**a** term that refers to a flaw in a system that can leave it open to **attack**. A **vulnerability** may also refer to any type of weakness in a **computer** system itself, in a set of procedures, or in anything that leaves **information security** exposed"



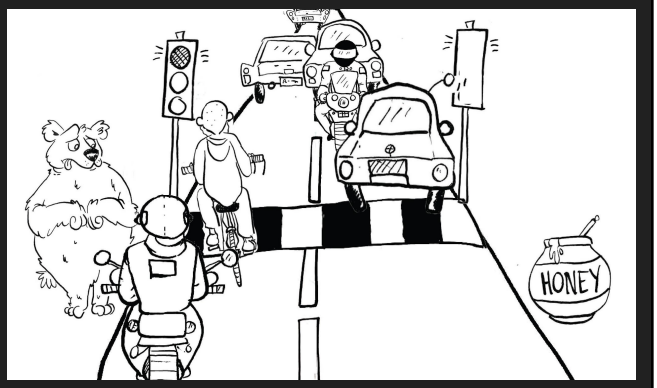
So the next part of the simple risk equation is (V)ulerbilites which are weakness, whether those are create through poor coding practices, flaws in the math used for encryption / cryptography (a good google search to start to look at that is ***vulnerability caesar cipher***)

So what are the vulnerabilities in the CiBear world?

The cyclist going through the red light as they are not following the procedure / law
The pothole in the road surface causing the car to go towards the bear
But did you spot the big one?
Yes the bear has soft tissue (it's fur, skin, etc) which is no match for the cars metal structure.

Likelihood

- Definition:
  - the chance that something will happen:
- Cyber example
  - the likelihood of a hacker attacking your system rather than someone else's



And the final part of the simple risk equation is (L)ikelihood, which is often very subjective and usually attracts debate about chance, probability etc.

In some industries like the vehicle insurance business there is actuary information that helps inform the likelihood, but there is not much information available to using in the Cyber business.

So what do we do with risks?

- We manage them in one of the following ways
  - **Avoid** – Change plans to avoid the risk;
  - **Control -** Change the risk result through reducing vulnerabilities or impact or likelihood or a combination of those;
  - **Accept** – Assume the chance of the the risk being realised is lower than the any of the other risk management options;
  - **Transfer -** to a third party

Broadly, there are four high level potential responses to manage risk, with numerous variations on the specific terms used to name these response options:

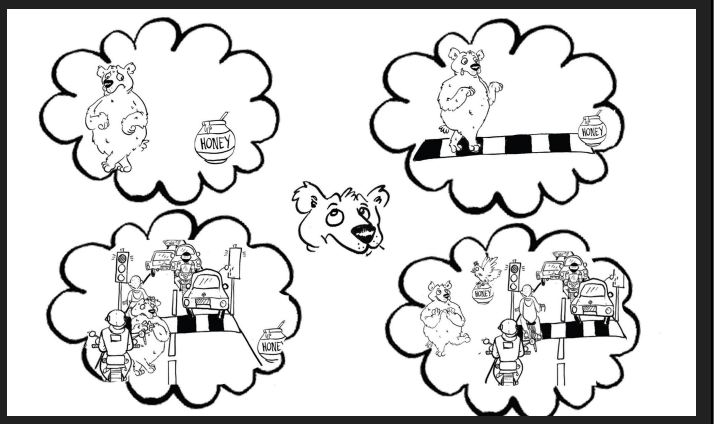
Avoid - for example don't provide an online retail service that process credit cards have customer post cheques
Control - put controls in place, for example encrypt credit card numbers whilst they are transmitted across networks to reduce the likelihood of disclosure, only store the last four digits of the credit card so if compromised the impact is less as they can't be used.
Accept - accept that doing business online has risks and that the benefits out weight the risks if they materialise
Transfer - outsource the risk around taking credit card payments to a third party for them to manage the risks or take out Cyber insurance.

It is useful to document the risks and the management decisions around the risks in a risk log of some kind which might state how long you will accept a risk until it is mitigated and when you should review risks that you have accepted.

The CiBear analogy - pulling it all together

So there is a risk that the bear cubs will starve if the CiBear crosses the busy road and gets hit by a fast car because he has soft fur and skin.

- Avoid - Don't attempt to get the honey from the pot
- Control - Use the pelican crossing
- Accept - Cross the road and hope a car does not hit him
- Transfer - send the chicken cross the road to get the honey pot



So this is the final slide in this deck and hopefully we have told the story well and pulled everything together?

So the risk (R=V*L*I) is the bear is vulnerable because it has soft tissue if it gets knocked down and dies the impact will be that it will not be able to provide for its cubs and the likelihood of him getting knocked down is high if there are a lot of cars travelling fast.

So the CiBear need to manage the risk we could just accept the risk and walk (if he ran he would be controlling the risk) across the road and hope that luck is on his side and no cars hit him.

He could use the pelican crossing and cross when the green bear lights up which is controlling / reducing the risk more that if he ran across the road, but a car could run the red light so there is still some risk there.

The CiBear could pay the chicken to cross the road (and the Chicken's risk control might be to fly over the cars)