Cyber by Sighbear
First Recap

How do Sighbear / Cyber bits fit together

v1.0

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

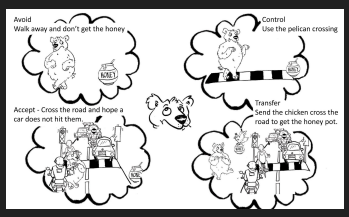
This slide deck summarises and adds a little bit to the first three Cyber Security slide decks, for those on the journey into Cyber and for those already in the industry, as to how and why we do Cyber Security.

This is the fourth slide deck and it is to help consolidate, before we move on to other topics.

Previously on SighBearUK Education

- If you have not seen part 1 to 3 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 covered CONTEXT.

- In the third deck we covered threat.

As the slide states this is a "previously on the SighBear Education"

This slide covers what the first three slide decks initially covered,

the slide decks with notes can be found at the following links.

- https://www.slideshare.net/Sighbearuk/cyber-bysighbear1-1notes
- https://www.slideshare.net/Sighbearuk/cyber-bysighbearcontext10notes
- https://www.slideshare.net/Sighbearuk/cyber-threatbysighbearnotes

The story today!

Introducing a few new terms and linking them together.

Today we are adding a few additional terms and linking things together.

We have covered these so far

- Asset - “something with value to someone / business”
- 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.”
- Capability - “the power or ability to do something.”
- Motivation - “a reason or reasons for acting or behaving in a particular way.
- Impact - the action of one object coming forcibly into contact with another.
- Vulnerability - The quality or state of being exposed to the possibility of being attacked or harmed.

This slide is a refresher of some of the terms we have mentioned so far.

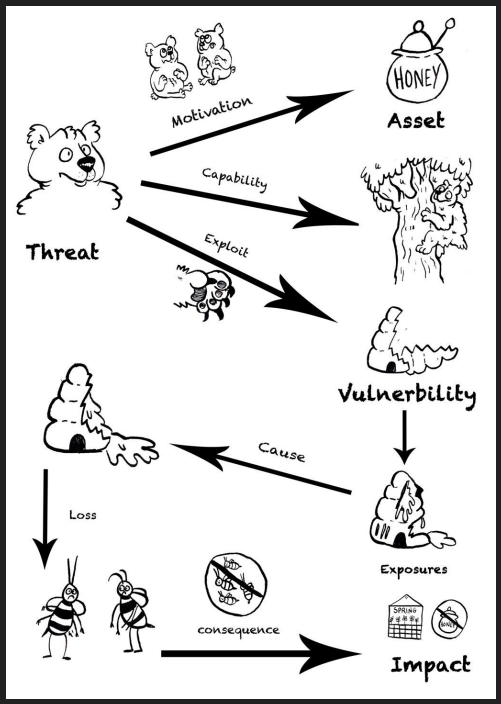
New(ish) terms

- Exploit - make full use of and derive benefit from.
- Cause - a principle, aim, or movement to which one is committed and which one is prepared to defend or advocate.
- Loss - the fact or process of losing something or someone.
- Consequence - a result or effect, typically one that is unwelcome or unpleasant.
- Exposure - the state of having no protection from something harmful.

This slide is covering a few new terms that fit / intermingle with the terms on the previous slides which we covered in other slide decks.

SighBear World

- A SighBear (Threat)
- wants to steal some honey (Asset)
- to feed to the bear cubs (Motivation)
- through using their skills for climbing trees (Capability)
- and using their claws (Exploit)
- to open bee hive (Vulnerability)
- which will (Exposure) the honey which will
- stop the bees having food stores (Cause)
- as the bear will steal the honey (Loss)
- bees will not survive the winter (Consequences)
- thus no honey next year (Impact) bears

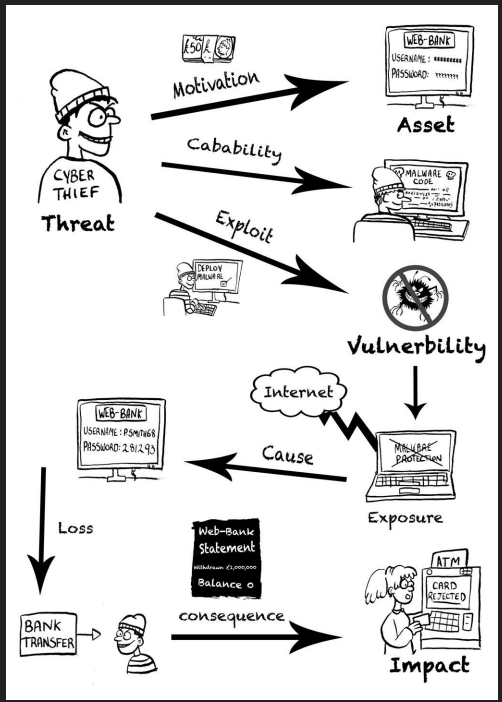


This is how the eleven defined words fit together in the Sighbear world

The Sighbear wants to steal some honey to feed to it's cubs, the Sighbear is great at climbing trees and has sharp claws that cut through beehives. Once the beehive is open the honey will be exposed and the bear can collect it for the cubs. This means the bees will not have any food for the winter and will not be around the following spring to make more honey.

Cyber world

- A cyber thief (Threat)
- wants to steal a user's banking credentials (Asset)
- to get money (Motivation)
- through using their skills to write malware (Capability)
- deploy malware (Exploit)
- and no malware detection (Vulnerability)
- which also leaves the device (Exposure) which will (Cause) credentials to be sent to the cyber thief
- which will allow the thief to logon as the user (Loss)
- and transfer money (Consequences)
- thus impacting (Impact) the user



This is how the eleven defined words fit together in the Cyber world

The Cyber Thief wants to get someone else's banking credentials so that he can transfer some money to himself. He knows how to write malware code and how to deploy that code, as some users don't protect their devices with malware detection and leave themselves exposed to attacks from the Internet. The deployed malware will capture the target's banking credentials and provide them to the thief, who can then use them to logon and transfer the money elsewhere. This means that when the target goes to get some money there is none left.

Credits

Thanks to all the CiBears and @DanielGDresner and @oracuk for input / reviews etc

Twitter @sighbearuk
web www.sighbear.uk

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

The Sigh Bear (UK) is all about educating the new CiBear cubs around cyber security through free and open source education and to give CiBear veterans a refresher of what constitutes a Pragmatic/Proportional Appropriate and Cost Effective (PACE) approaches to cyber related topics.

A long time ago, in a galaxy far, far away… the light side of the force suffered a data breach of the worst and most catastrophic kind possible, the designs for the passwordless authentication were stolen by the dark side of the force.

So when the light side rolled out the passwordless authentication to the universe, the dark side already had exploits to deploy against the vulnerabilities in the passwordless authentication leaving it's systems exposed to the dark side of the force.

So if you're on the light side of the force try to think like someone on the dark side to help build and defend systems better.

Plagiarized / based on https://www.huntsmansecurity.com/blog/cyber-security-quotes-lessons-in-movies-episode-1/