Cyber by Sighbear
Context is Key

What are the CiBears without context?

V1.0 (Copyleft)

Any comments / suggestion / abuse tweet @SighBearUK

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

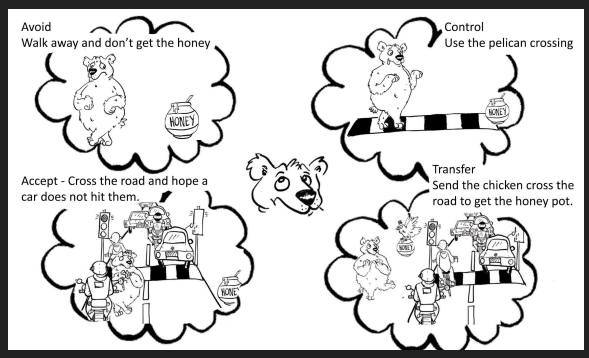
This slide deck expands on the initial story of Cybersecurity and continues the journey for those who wish to get into the industry and as a refresher to those already in the industry as to how and why we do Cyber Security.

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

The story so far

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

- In the first slide deck we covered Cyber & Risk.
- Then we joined the two together for Cyber-Risk.
- We used Cyber and CiBear world examples to help introduce a simple equation for risk assessment.
- The deck introduced each of the parts to the equation.
- It finally wrapped it up with risk management.



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

We joined Cyber and Risk together for Cyber-Risk.

The deck then used Cyber and CiBear world scenarios whilst introducing a simple risk equation (R = V * L * I) for risk assessment.

Then it introduced each of the parts to the equation, R=Risk, V=Vulnerability, L=Likelihood and I=Impact (which also covered assets and value).

The deck finally wrapped it all up with risk management through the following approaches

- Avoid
- Control
- Accept
- Transfer

The story today!

CONTEXT! - Introduce it

As it says on the slide.

What is context?

- **Context is Key**
- Definition of Context
  - “the circumstances that form the setting for an event, statement, or idea, and in terms of which it can be fully understood.”

Understand the context.

What is the context, what are you trying to achieve and what are the parameters that apply?

Hopefully the next few slides answer this question.

Why apply context in the Cyber world?

Cyber world

A business is thinking of deploying a new IT system

- Where should they deploy?
- On premises or in the Cloud?

So when applying cyber-risk you need to understand what the business is trying to achieve and how they might want to achieve it, which will then have an effect on the risks.

Remember the equation from the first slide deck?

R = V * L * I (R=Risk, V=Vulnerability, L=Likelihood and I=Impact)

These will change based on the context.

For example, if the location of the information stored on premises is on a fault line then the likelihood of a earthquake increases, this needs a context driven risk approach.

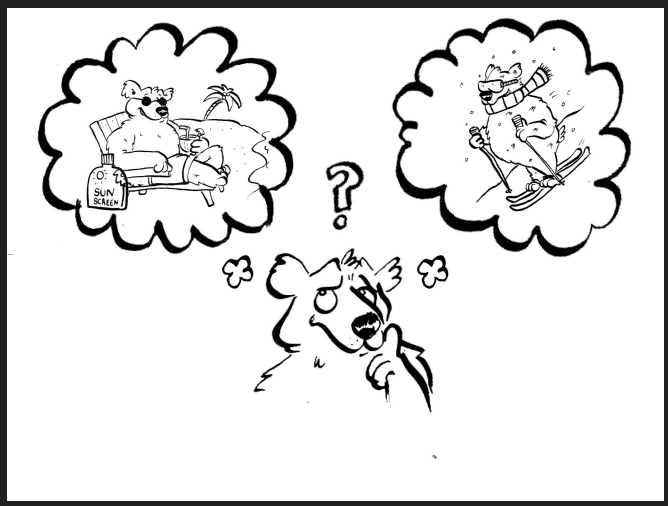
Can you work out what 1001101000010 is?

Why apply context in the Sighbear world?

Sighbear world

The bear is thinking of going on holiday

- Where should they go?
- Somewhere cold or hot?



So when Sighbear is thinking of going on holiday he applies a risk approach, you need to understand what the bear is trying to achieve (sun tan or adrenaline seeking) and how he wants to achieve it which will then have an effect on the risks.

Remember the equation from the first slide deck?

R = V * L * I (R=Risk, V=Vulnerability, L=Likelihood and I=Impact)

These will change based on the context.

For example if the holiday destination has a heightened likelihood of terrorist activity, or kidnap etc, these need context driven risk approaches.

Applying context in the Sighbear world?

Hot holiday, have some shade.

Cold holiday, why have some shade?

So if the Sighbear goes on holiday to a hot destination (the context).

R = (V = Bear's fur) (L = Sun is hot) (I = Overheating / dehydration)

"There is a risk that the sun will be hot leading to an impact of dehydration, due to thick fur which could be mitigated by staying in the shade". The shade would be a risk management option under control (controls will be covered in later slide decks).

If the Sighbear goes on holiday to a cold destination (a different context).

What is the point of having some shade?

This is why context is key/king (or queen or ….).

Another context example.

The Sighbear is in the freezing North pole and could put on hat, gloves and scarf if it wants to go outside its warm igloo that has a fire, or it could just stay inside thus avoiding the risk of freezing.

He might need to apply sun cream on both hot and cold holidays as the sun can burn even in cold climates.

Applying context in the Cyber world

New IT system on premises - install CCTV, Locks, Security guards, etc

New IT system in the cloud - apply countermeasures that the business is responsible for.

So if the business wants to deploy to the cloud (the context)

R = (V = mis-configuration) (L = hackers target the clouds) (I = information compromised)

"There is a risk that the hackers will mount a successful attack leading to an impact of information being compromised.
Due to the business not understanding it's cloud responsibilities (i.e. exposing the database tier to the Internet with a simple guessable password).
Which could be mitigated by reading and understanding the cloud responsibility model"

The cloud responsibility model would be a risk management option under control (more information on controls (which is not the same as control option in Cyber-Risk management) / countermeasures will be covered in later slide decks).

But if the business wants to deploy on premises (a different context)

What is the point of them understanding the cloud responsibility model if they are not using the cloud?

This is why context is key/king

Another context example

R = (V = no physical security) (L = criminal) (I = information compromised)

"There is a risk that a criminal will steal equipment leading to an impact of information compromise, due to the business not having any physical security controls for where the system is housed (i.e. doors without locks, etc) which could be mitigated by applying some physical controls"

Some of the countermeasures that could be deployed are:

- Avoid - Put system in a hosting data centre (which will also have some transfer element to it)
- Control - Add locks to doors, CCTV, etc
- Accept - Hope a criminal does not target you
- Transfer - Contract a security firm to provide guards

(as mentioned more information on countermeasures will be covered in later slide decks).

Question?

So if you have a computer on a desk in a secure office that is unlocked but there is CCTV, security guards, biometric access control on the doors etc (which is a really visible risk) vs a webserver on the Internet that has never been patched with no firewall (not as visible risk), which should you address and why?

Answer
Depends on the context; what is on the web server? Maybe it is a Honey Pot!

Bonus Question?

Why is the Sighbear at the job centre?

Answer

Because under the cloud shared responsibility model the cloud provided takes care of the physical security (the risk from physical attacks has been transferred to them).

And finally.

There are some size 11 shoes for sale on the Internet - will they fit you?
What size are you feet?
Are these child size 11 or adult? So the context here might be which section of the online shop they are in, adult or children's.

Bear traps

- Think about scenarios but avoid the never ending ifs.
  - (if an attacker, got into the build and if that attacker had credentials and if they bypassed the biometrics, if…….).

Think of plausible scenarios, i.e. a user uses a weak guessable password, firewall allows all inbound (ingress) and outbound (egress) traffic.

Try to avoid going down the if & if & if rabbit holes…...

We often hear things like,

If the attacker fakes a building pass, copies some biometric (jelly baby attack or Gummy Bear attack) https://www.theregister.co.uk/2002/05/16/gummi_bears_defeat_fingerprint_sensors/), pays the security guards, stands on one leg etc then they might just be able to compromise the asset.

Context is Key, Context is King (or queen or ……..!

More Bear traps

- There is no such thing as one size fits all in Cyber risk.
  - The business does not need to employ a physical security guard for protecting the cloud.
- Tick/Checkbox exercise can lead to false sense of security.

One size of countermeasures does not fit everything.

Example one:

Policy states a requirement to physically lock computing devices to a desk. Hard to do with a mobile phone or a server; it is all about context. Most likely servers are in a computer hall with different controls to a phone that might have a biometric lock and, as it states, it is mobile so you are likely to have it in your pocket/bag rather than left on a desk.

Example two:

Countermeasures to protect all data/information transmitted and stored must be encrypted with FIPS140-3. Lots of systems / products don't support the FIPS (Federal Information Processing Standard) plus sometimes the no FIPS version maybe safer. (https://www.yubico.com/support/security-advisories/ysa-2019-02/)

Often businesses will state they comply to a standard (ISO/IEC 27001) or framework (COBIT (Control Objectives for Information and Related Technologies)) but:

1. What is the scope / context of how they are applied?
2. Were all the countermeasures used or just those to support risk management?
3. Does anyone check the countermeasures?
4. Do they mean comply or are they certified against by an independent external audit?

Context is Key, Context is King (or queen or ……..!

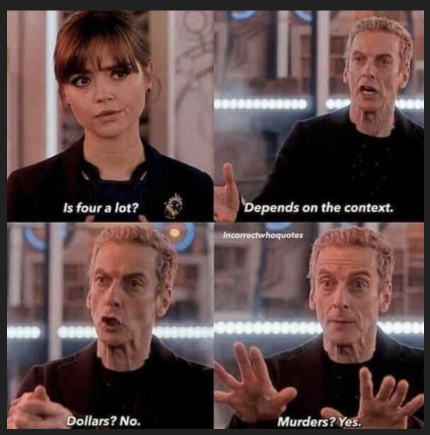
Summing up and what's coming next

Summary - Hopefully this slide deck explains / shows why context is very important and why not to just apply all countermeasures everywhere.

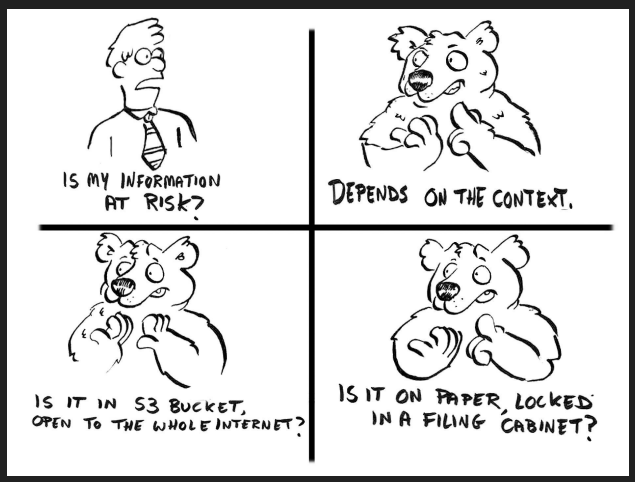
Coming soon - we will expand on the risk equation and countermeasures.

Hopefully this slide speaks for itself?

Graphical representations



Credit - @warmana



Hopefully you get the pictures?

Context is vitally important for everyone……

Including security!

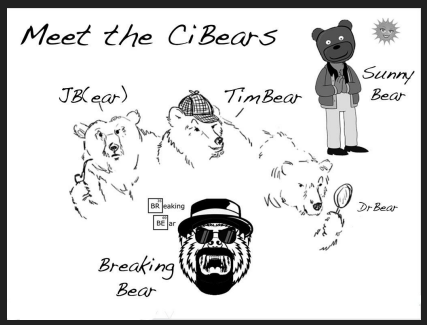
Hopefully this does not need any speaker notes?

Credits

If you have a cyber challenge, if no one else can help, and if you can find them, maybe you can hire the **CiBears?**

https://twitter.com/sighbearuk

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



Just in case you are too young to remember the A-Team?

https://www.imdb.com/title/tt0084967/quotes

"10 years ago a crack commando unit was sent to prison by a military court for a crime they didn't commit. These men promptly escaped from a maximum security stockade to the Los Angeles underground. Today, still wanted by the government, they survive as soldiers of fortune. If you have a problem, if no one else can help, and if you can find them, maybe you can hire the A-Team."

The CiBears blatant rip-off

3 years ago a crack bear unit was sent to deepest darkest Peru by a UK court for a crime they didn't commit. These bears promptly escaped from a maximum security cage to the Cyber underground. Today, still wanted by the government (to help them), they survive as bears of fortune. If you have a problem, if no one else can help, and if you can find them, maybe you can

hire the CiBears.