

DAVE ON CYBER PRESENTS

Domain 1, Booklet 4

CISSP as an Art

RISK ASSESSMENT

WITH

UV



RADIATION

created by Dave Krunal



Dad, why skin cancer rate is higher in Australia?

Johnny,
I just came
from office.
Give me a second





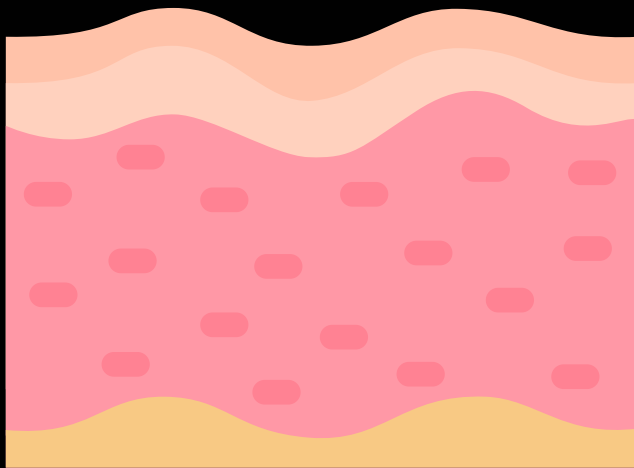
Ok, one second is
over. Now tell me,
why?

It was an
expression, Johnny.
Well,
let me explain.



IT'S HAPPENING...

Australians suffer highest skin cancer in the world. Each year, around 1200 people die from skin disease.



It's linked to UV Radiation which happens because of depletion of Ozone layer near south pole.

OH NO...



It's scary Dad!

What's going to happen?

I don't want to go to
beach anymore.

Can we move from Australia?

CALM DOWN SON...

THERE IS A WAY



? Please tell me dad.

I can't wait to know more.

Is it some kind of magic?

NOT MAGIC, SON.

BUT, A QUANTITATIVE RISK ANALYSIS

LET'S BEGIN...

We love spending time with friends and family on beach during summer.



We need to be aware that UV rays without Ozone layer is risk to our body.

OUR BODY IS OUR ASSET.

AV - ASSET VALUE

Every asset has an value.

Example, a web server as an asset may cost \$200,000 for its maintenance, operational cost, licensing and support.

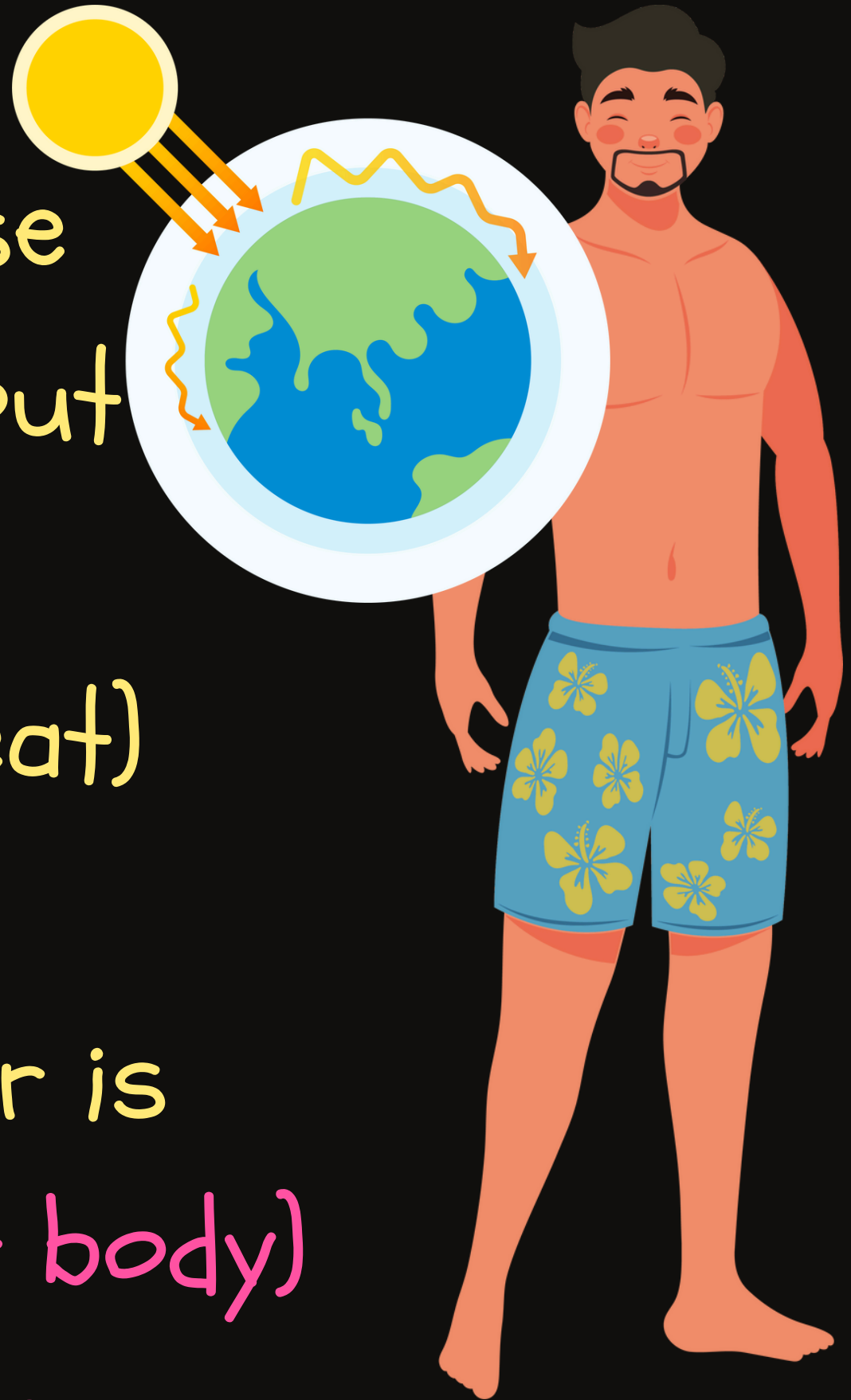
So, asset value (AV) = \$200,000

If human is an asset, optimistically we live up to 130 years. So, AV = 130

YOUR BODY AS THE EXPOSURE

When you expose
your body without
protection to
UV Radiation (threat)
in area

where Ozone layer is
depleting - you (your body)
are the exposure.



EF - EXPOSURE FACTOR

No asset is 100% secure.

Every asset has some kind of exposure factor (EF) from threats or zero-day attacks.

If our \$200k web server in data centre has 45% chance of fire, then EF is 45%.

EF is nothing but loss of percentage from realised risk.



Dad, what do we with asset value (AV)
and exposure factor (EF)?



It helps you to find
SLE - single loss expectancy.



English dad. And I'm 7 years old!



Ha ha! I was joking Johnny.
Let me explain...

A LOT CAN HAPPEN ON SUNNY DAY

Consider human lives up to 130 years. And UV rays exposure on a specific day is 50%.



Asset value (AV) = 130 years

Exposure Factor (EF) = 50% UV

Single Loss Expectancy = AV * EF

SLE = 130 * 50%

SLE = 65 years

A single exposure event could theoretically reduce the body's lifespan by 65 years.

SINGLE LOSS EXPECTANCY (SLE)

In the human body analogy, SLE represents the amount of lifespan lost in a single damaging event, which is the result of the body being exposed to harmful UV rays.

Let's calculate same for our web server.

$$SLE = AV * EF$$

$$SLE = \$200,000 * 45\%$$

$$SLE = \$90,000$$

A single DDoS attack could cause \$90,000 in losses to the web server, considering both downtime and recovery costs.

WHAT ARE THE ODDS?



I want to live longer, Dad
I'm not going out in summer.

Oh C'mon Johnny.
Everyday won't be like that.



There are usually 10% of days when human body
is exposed to harmful UV rays.

That's the concept of
ARO - Annualized rate of occurrence

ARO - ANNUALIZED RATE OF OCCURRENCE

The Annualized Rate of Occurrence (ARO) is the estimated frequency at which a damaging event (such as UV exposure) occurs within a year.

If human is exposed to harmful levels of UV rays 10% of the time - one exposure every 10 years.

$$1/10 = 0.1$$

ARO is 0.1

CALCULATING ARO FOR WEB SERVER

If the web server faces a DDoS attack once (one attack) every five years, the ARO would be 0.2

$$1/5 = 0.2$$

Remember

ARO could be zero if threat or risk is never realised. In that case,

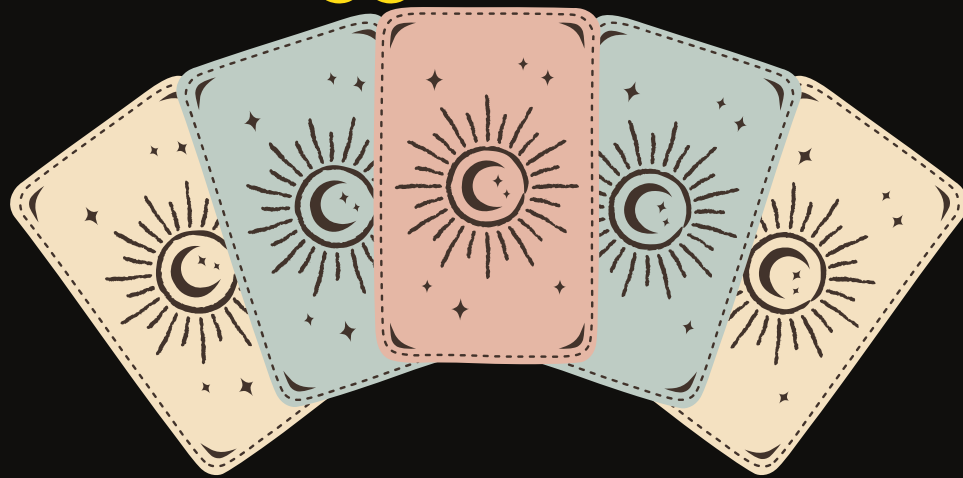
ARO is zero.

GET THE BIGGER PICTURE



Ok I got it so far
But what we will do with
all that ARO and SLE?

To get a bigger picture, Johnny



IT KIND OF PREDICTS THE FUTURE!

That's the concept of
ALE - Annualized Loss Expectancy

PREDICTING THE FUTURE

If you go out in the sun with high UV rays,
without protection...



On average, the person
might lose 6.5 years
of lifespan
annually due to
UV exposure.

$$\text{ALE} = 65 \text{ years} \times 0.1$$

$$\text{ALE} = 6.5 \text{ years per year}$$

ANNUALIZED LOSS EXPECTANCY (ALE)

The Annualized Loss Expectancy (ALE) is the total expected loss over a year, considering the frequency of the event.

With our web server -

$$ALE = SLE * ARO$$

$$ALE = \$90,000 * 0.2$$

$$ALE = \$18,000$$

The web server can expect annual losses of \$18,000 due to DDoS attacks, based on the frequency of attacks and the expected damage from each incident.

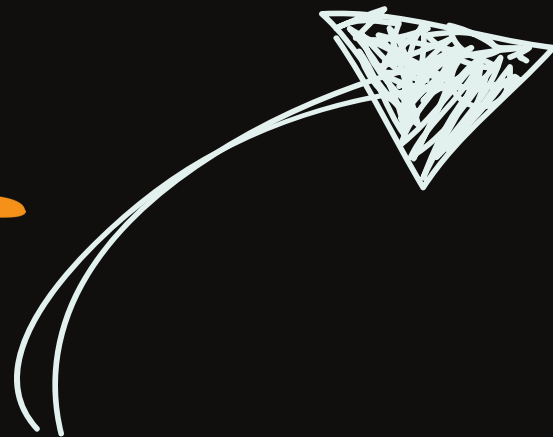
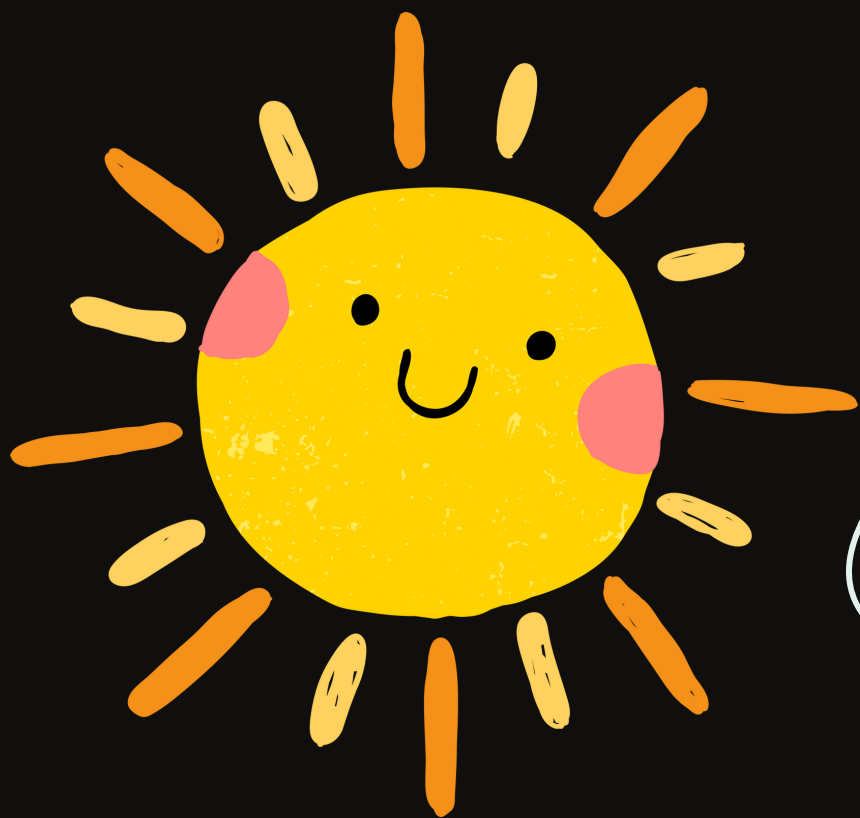
WHAT TO DO?



Awesome!

Now, what can I do for the protection?

Apply sunscreen with sun protection factor (SPF). It filters 98% of UV radiation.



NEW EF AND ALE

Applying sunscreen as a safeguard reduces the exposure factor from 50% to 10%

ALE before sunscreen = 6.5 years per year

SLE after sunscreen = 130 years * 10%

SLE = 13 years

ALE after sunscreen = 1.3 years per year

Now person loses 1.3 years annually due to UV exposure when using sunscreen.

SAFEGUARD COST

Safeguard implementation is necessary but...



The purpose of safeguard is to reduce the ARO. However, the cost of safeguard and related costs should be considered.

Remember

IF THE COST OF SAFEGUARD IS

GREATER THAN ASSET VALUE, YOU

SHOULD ACCEPT THE RISK.

What does that mean Dad?



200 YEARS OR 65 YEARS?



**TURN ON YOUR HYPOTHETIC MODE AND
IMAGINATION, JOHNNY**

Human lives up to 130 years. What if
person now spends the equivalent of
seven years of their lifespan annually on sunscreen?

Net benefit = ALE before safeguard - ALE
after safeguard - Annual cost of safeguard

Net benefit = 6.5 years - 1.3 years - 7 years

Net benefit = -1.8 years per year



The net benefit is only -1.8 years per year.

It's kinda you die before you live.

HA HA HA!

IT'S NOT WORTH DAD!

I'd rather live 65 years
and enjoy my life



SPOT ON, JOHNNY

IT WAS JUST AN EXAMPLE!

Let's understand this cost/ benefit
formula and numbers with our
web server scenario

THE NEW ALE IS GOOD BUT...

If the annual cost of the safeguard was higher than the asset value or risk reduction, it would make sense to accept the risk rather than applying the safeguard.

ALE before DDoS protection = \$18,000

ALE after DDoS protection = \$4,000

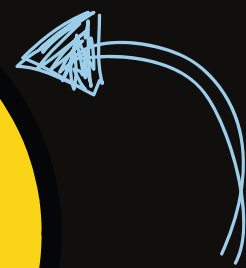
ALE looks awesome but there are two options after we take annual cost into the account for the net benefit.

OPTION 1 - POSITIVE

Net benefit = ALE before safeguard - ALE after safeguard - Annual cost of safeguard

$$\text{Net benefit} = \$18,000 - \$4,000 - \$10,000$$

$$\text{Net benefit} = \$4,000$$



security team!

THE SAFEGUARD RESULTS IN A NET BENEFIT OF \$4,000 PER YEAR, MEANING IT IS WORTH IMPLEMENTING THE SAFEGUARD SINCE IT SAVES MORE THAN IT COSTS.

OPTION 2 - NEGATIVE

Net benefit = ALE before safeguard - ALE after safeguard - Annual cost of safeguard

Net benefit = \$18,000 - \$4,000 - \$20,000

Net benefit = -\$6,000



security team!

IMPLEMENTING THE SAFEGUARD RESULTS IN A NET LOSS OF \$6,000, MEANING IT'S MORE COST-EFFECTIVE TO ACCEPT THE RISK AND HANDLE THE OCCASIONAL DDOS ATTACKS MANUALLY OR THROUGH LESS COSTLY MEANS.

CISSP CORE CONCEPT

$$SLE = AV * EF$$

$$ALE = SLE * ARO$$

ALE 1 - COST PRE IMPLEMENTING SAFEGUARD

ALE 2 - COST POST IMPLEMENTING SAFEGUARD

ACS - ANNUAL COST FOR SAFEGUARD

$$\text{BENEFIT} = ALE 1 - ALE 2 - ACS$$

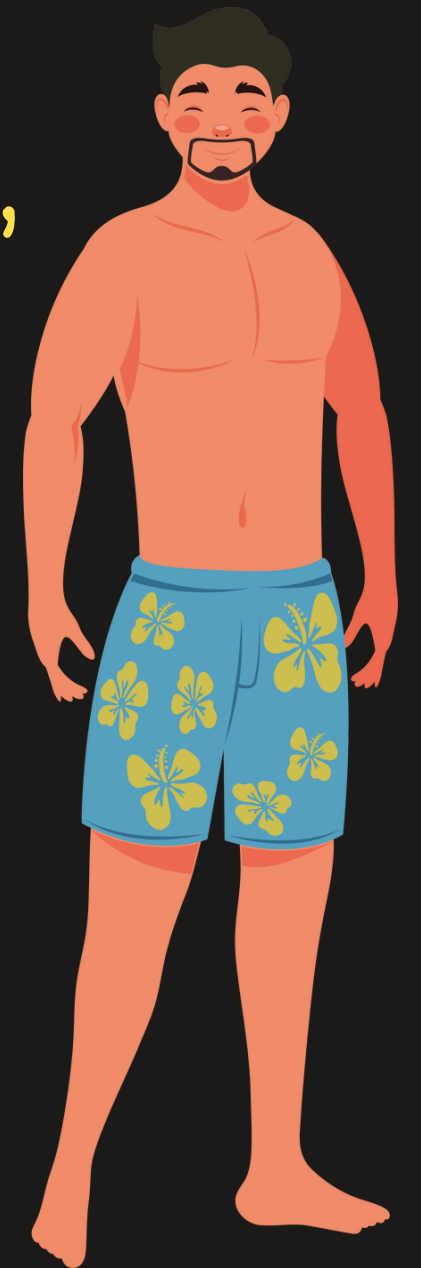
REMEMBER!

BEACH TIME!!



WAIT FOR ME JOHNNY,

I'M COMING...



DAVE ON CYBER PRESENTS

CISSP as an Art Series

created by Dave Krunal

I hope you enjoyed this creative CISSP booklet. I'd love to connect and hear you feedback on my work.

SUBSCRIBE - [DAVEONCYBER.COM/SUB/](https://daveoncyber.com/sub/)

CONNECT - [LINKEDIN.COM/IN/DAVEKRUNAL/](https://www.linkedin.com/in/davekrunal/)

EMAIL - [DAVEONCYBER@GMAIL.COM](mailto:daveoncyber@gmail.com)

WEBSITE - [DAVEONCYBER.COM](https://daveoncyber.com)