

STORIES FROM THE

# DARK SIDE





**KYLE IN  
THE YOUTH**

*LIKES BREAKING THINGS*

@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

NO PROBLEM ON TIME OF DELIVERY

NO RESTRICTION OF AGE

NO RESTRICTION ON OPENING HOURS



FOLLOW THE

MONEY\*



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

\* 2022: 207 BIL. € (DE ONLY)

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



THE MATHS BOOK

IT'S A TRAP!

100 % SUCCESS RATE

SPEARING

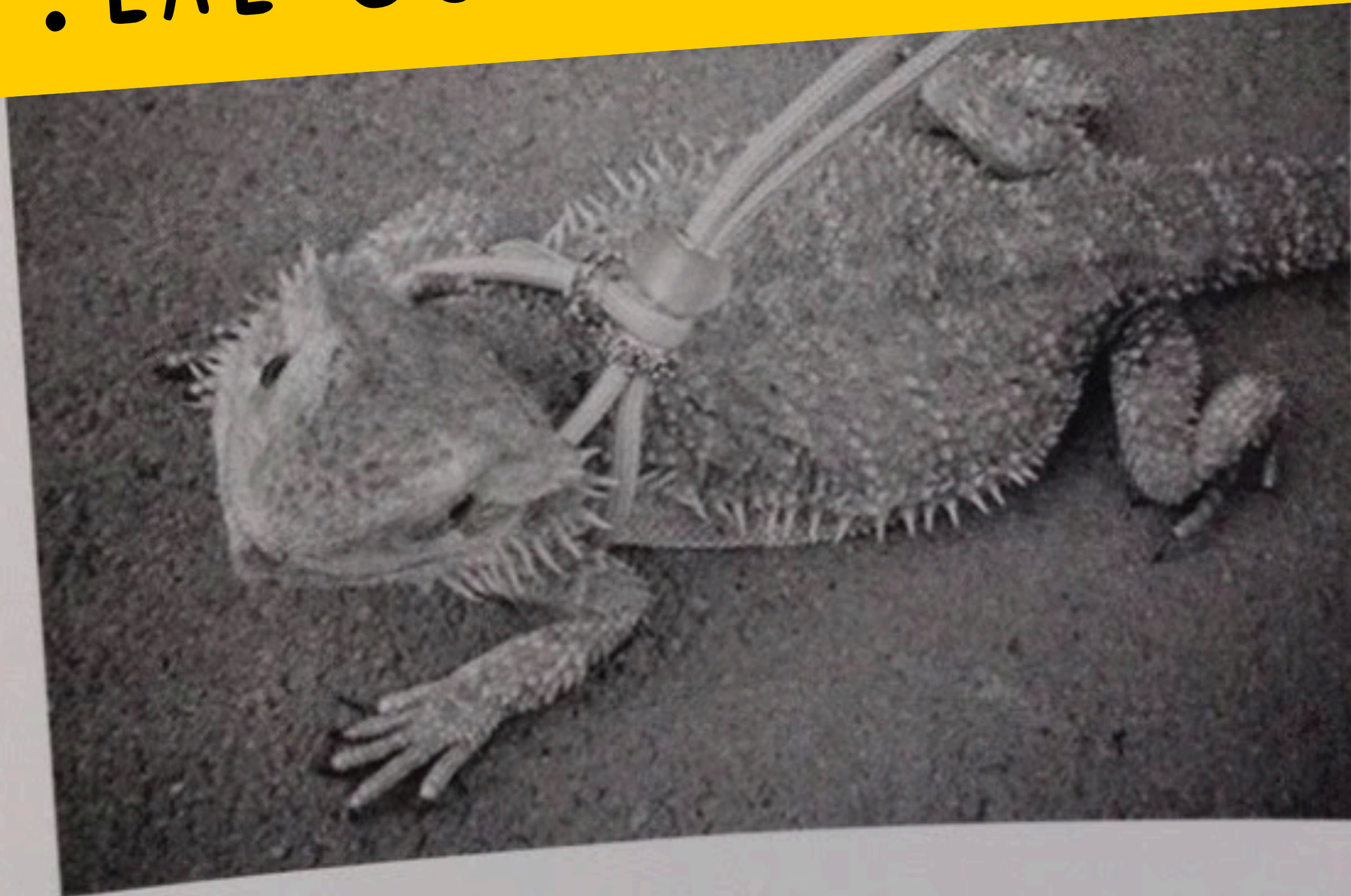
PHARMING

VISHING

WHALTING



. 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  
DSCVO

EXTORTION  
RELEASE

RANSOM  
ENCRYPTION

EXTORTION  
REPUTATION

RINSE AND  
REPEAT

...

TYPICAL

\* CYBER CYBER

# KILL CHAIN\*

MEAN TIME TO

BREACH

< 24 H\*

\* TO DOMAIN ADMIN

\* LATERAL MOVEMENT

\* EXFILTRATION



THE DAMAGE



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

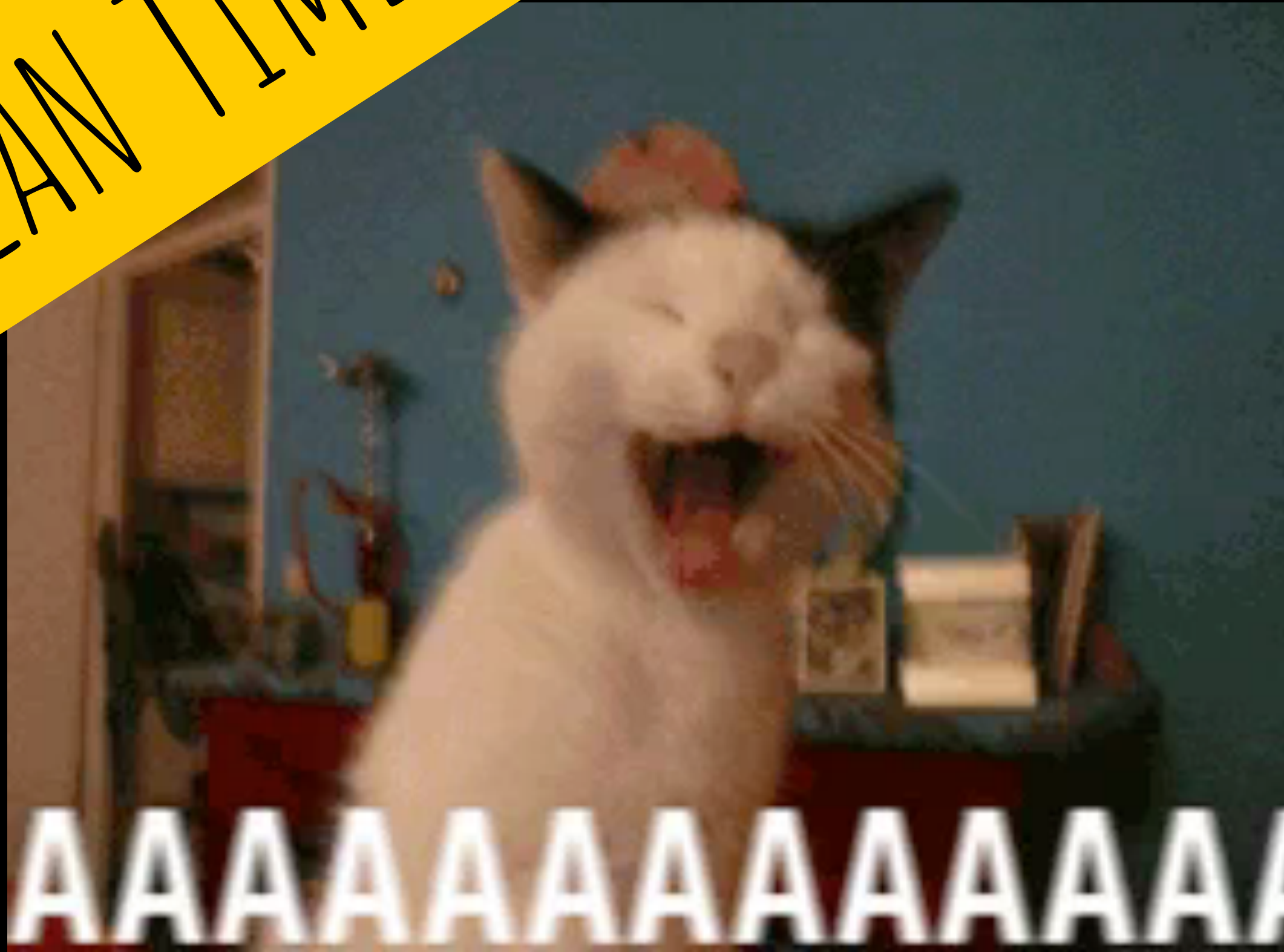
MORE THAN 52 DAYS

\* YOUR PROBLEM IS NOT TECHNICAL

\* YOU SHOULDN'T DO  
IT AT ALL



MEAN TIME TO



\* 270 DAYS

\* IT'S BAD

\* REALLY BAD

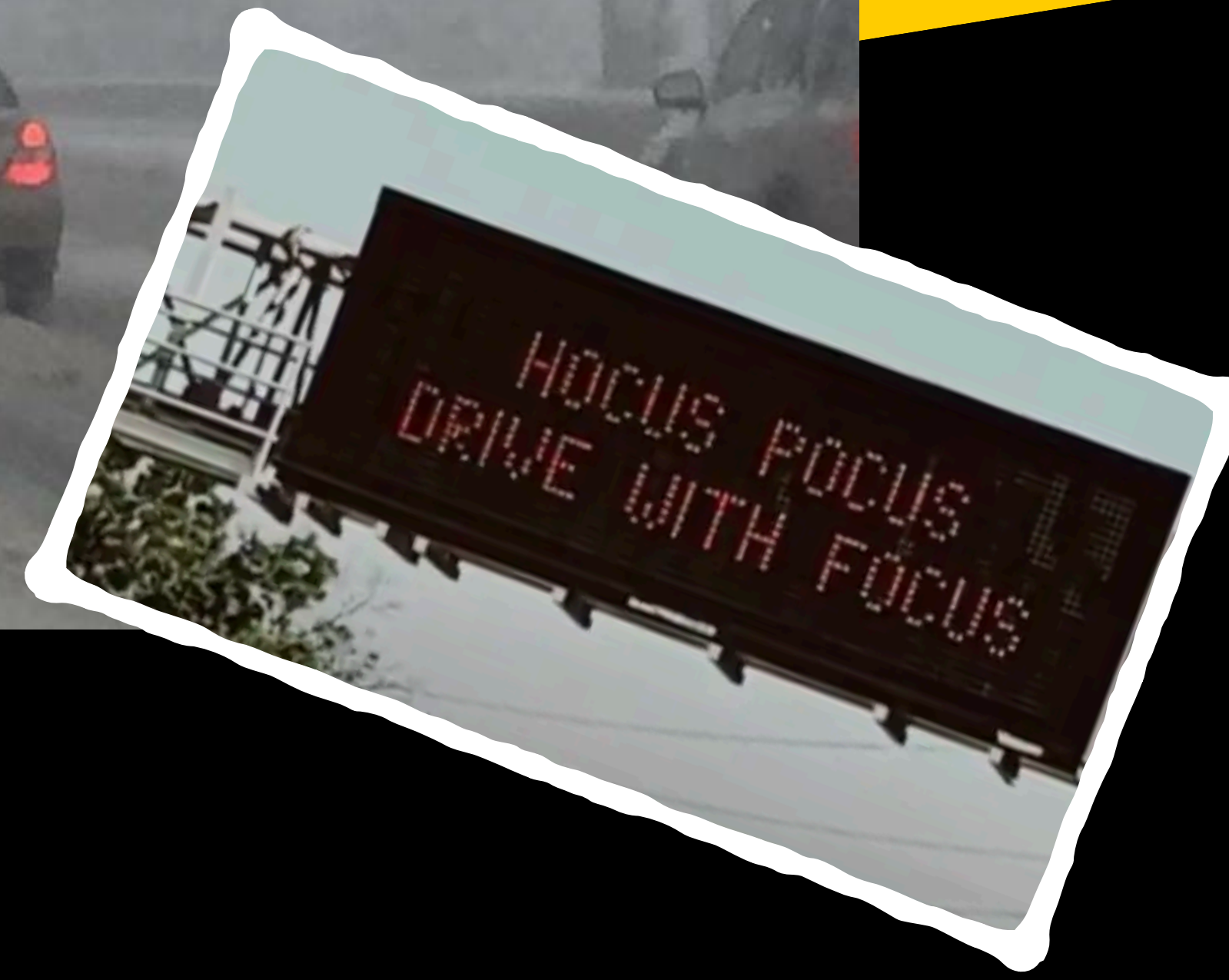
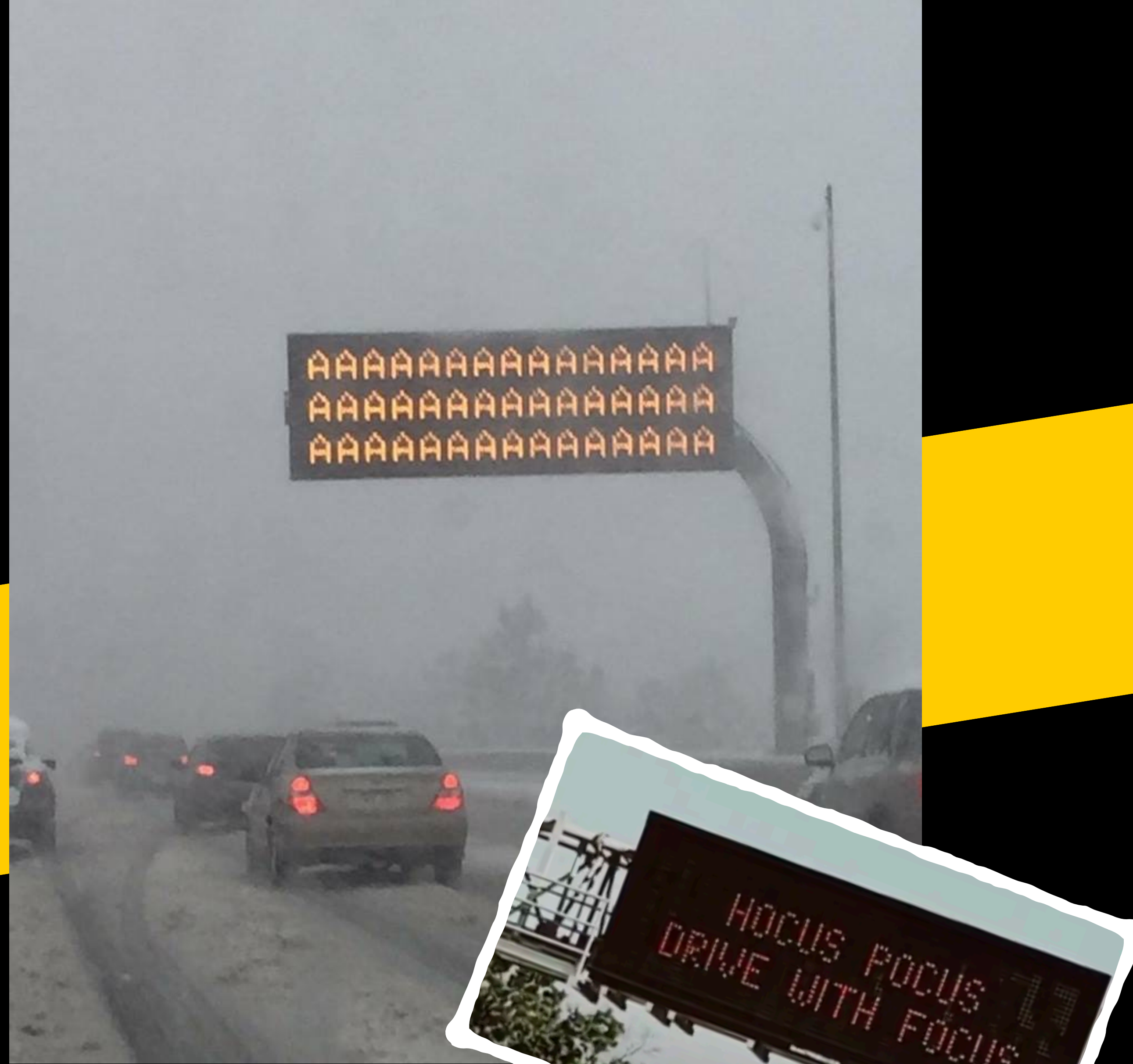
\* REALLY REALLY  
BAD

**CONT** AAAAAAAAAAAAAA **IN**

WHAT COULD

POSSIBLY

GO WRONG ?





xkcd #327

LITTLE **BOBBY** TABLES

**THE CAUSE**

MANAGEMENT

VS.

CYBER SECURITY

WE ARE **TAKING**  
THAT RISK!







CYBER RISK  
ASSESSMENT  
FOR

LOOSERS\*

\* YOU WILL LOOSE THIS RACE

\* YOU DO TOO LITTLE TOO SLOW



"THATS OUT OF  
SCOPE!"

- SAID NO ATTACKER EVER

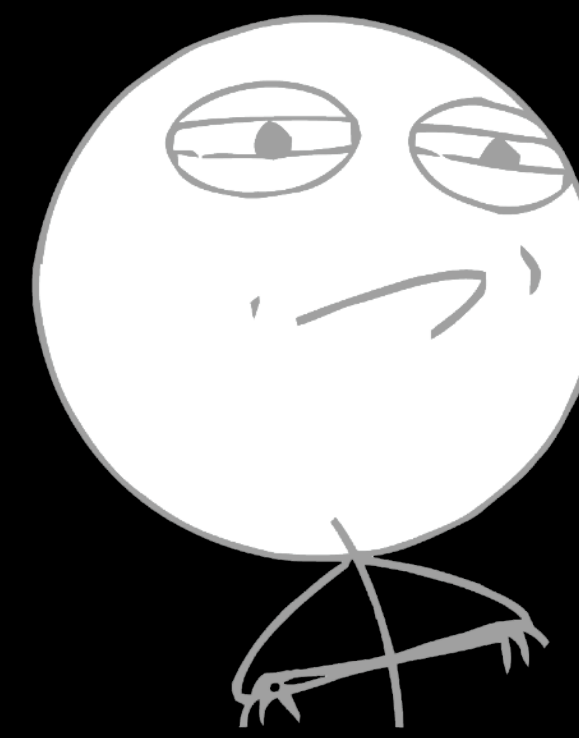
AND INSTANTLY  
YOU'VE GOT  
SHARKNADO

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!



BUT AI

WILL FIX 'EM

NOPE.

LIE.

YAST.

NEA.

ILLUSION OF  
SECURITY

NOTIFYING LIBERATES

DOCUMENTATION  
OVER FIXING

I  
S  
O

2

7

0

0

1

WE'RE FINALLY SECURE

I CHECKED ALL THE  
BOXES

THE SOLUTION



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.**