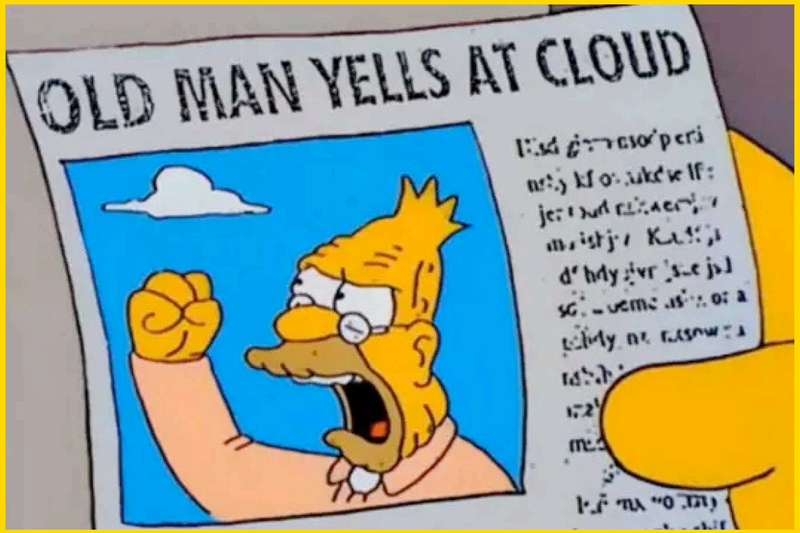
Be Better At Infosec - Lessons learned over an eternity.

Sept 16,2021



As is customary…

All views expressed in this presentation are my own and

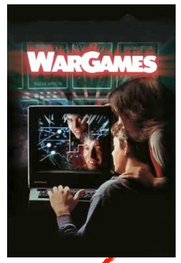
not those of my company.

However, since I work for my own company…maybe not.

There are some generalizations in here though….just to be clear.

Obligatory bio slide

1973



Do interesting things

1981

1984

1989

1992

(Business job) KPMG

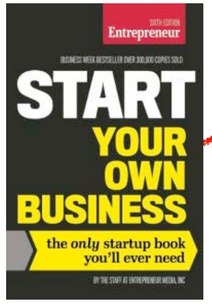
1997

2001

2005

(Politics job) UBS

CMC cmc markets (MacGyver job)



2010

2012

2021

2024

World Saved. Job done.

Platform launched

Note: Accent goes astray somewhere

What are we talking about?

Stuff that would have been useful to be told when I started doing this...

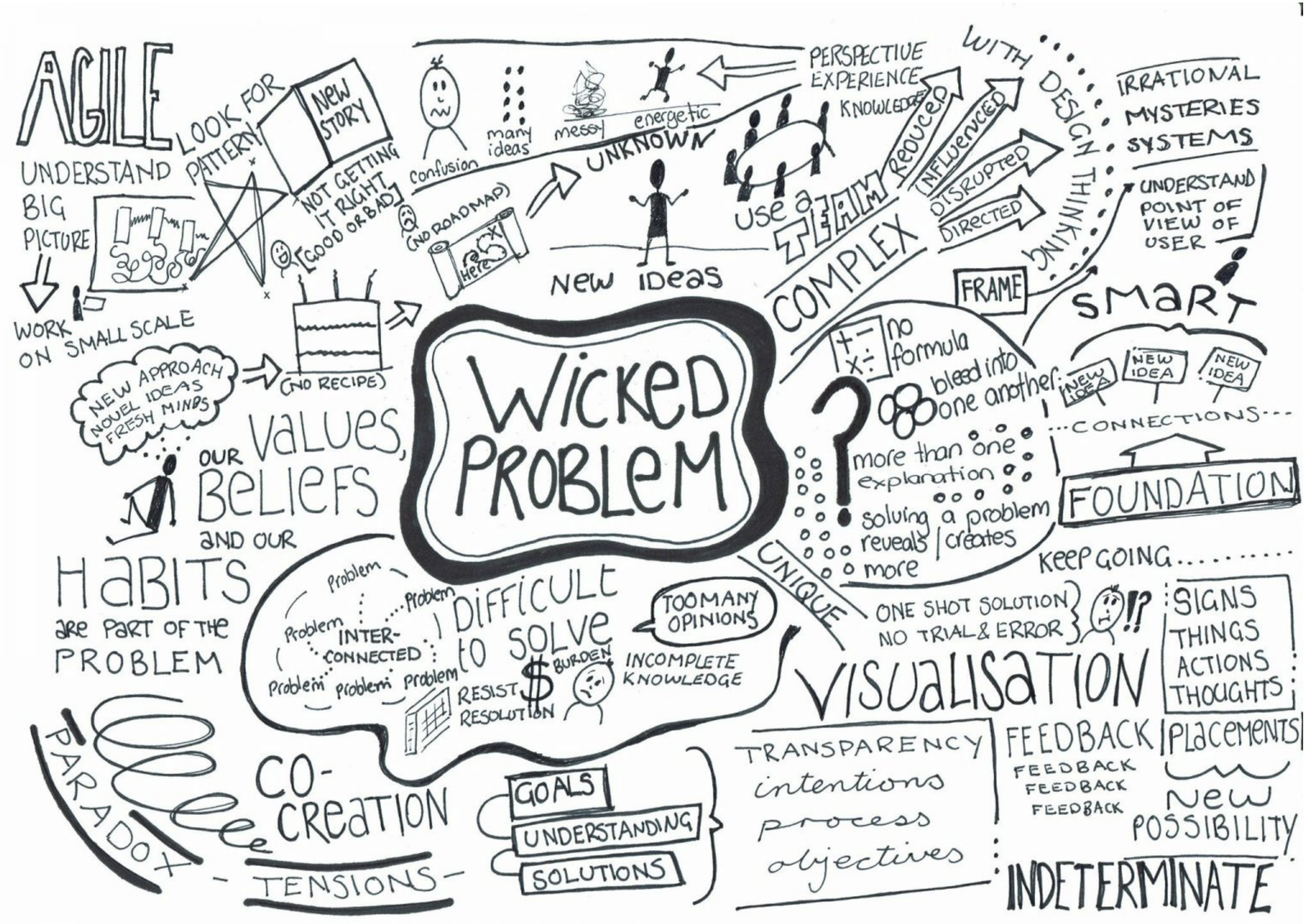
Infosec often feels like..

Hopefully some of the info that follows

will help you out.

If nothing else, It may save you your hair...

Lesson 1: Its Complicated



Lesson 2: Mostly useless things

(That we nonetheless have to do)

Installing AV	Security Awareness	Vendor Reviews
“Black box” Testing	Compliance	Reviewing “threat Intel”

Lesson 3:Auditors are not evil

Work with them

Budget approval?

Boss happy

Promotion

Work against them

Missed targets

Problems for boss

Job loss (yours)

*** There are exceptions in which case go to plan B.**

Lesson 4: Don’t just rely on tools

If you do then you may..

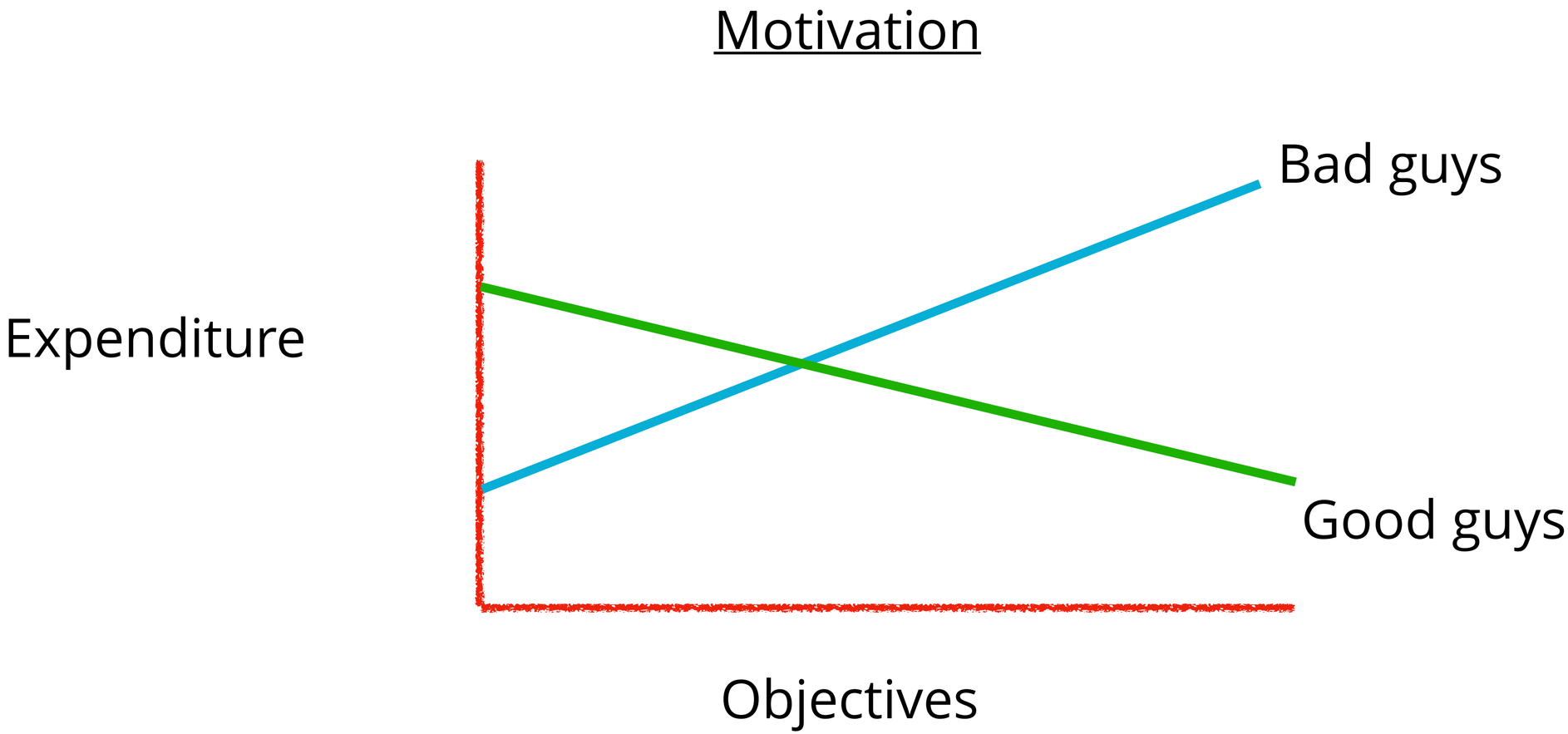
- Suffer outages - Wait, I can’t scan that with Nessus?
- Create a false sense of security - The scans found nothing, we are safe!
- Be out of a job - if all you do is run tools, how about we automate those? Outsource it?

Instead...

- Learn the “core stuff” - TCP and other networking, operating system fundamentals, some programming, Database fundamentals, how stuff actually works.
- Roll your own distro
- Manual testing

Lesson 5: Don’t underestimate the bad guys

They keep breaching environments, thinking “outside the box” and finding bugs.



Lesson 6: One size never fits all

Your organisation actually is a unique and beautiful snowflake

Would not be a good CISO

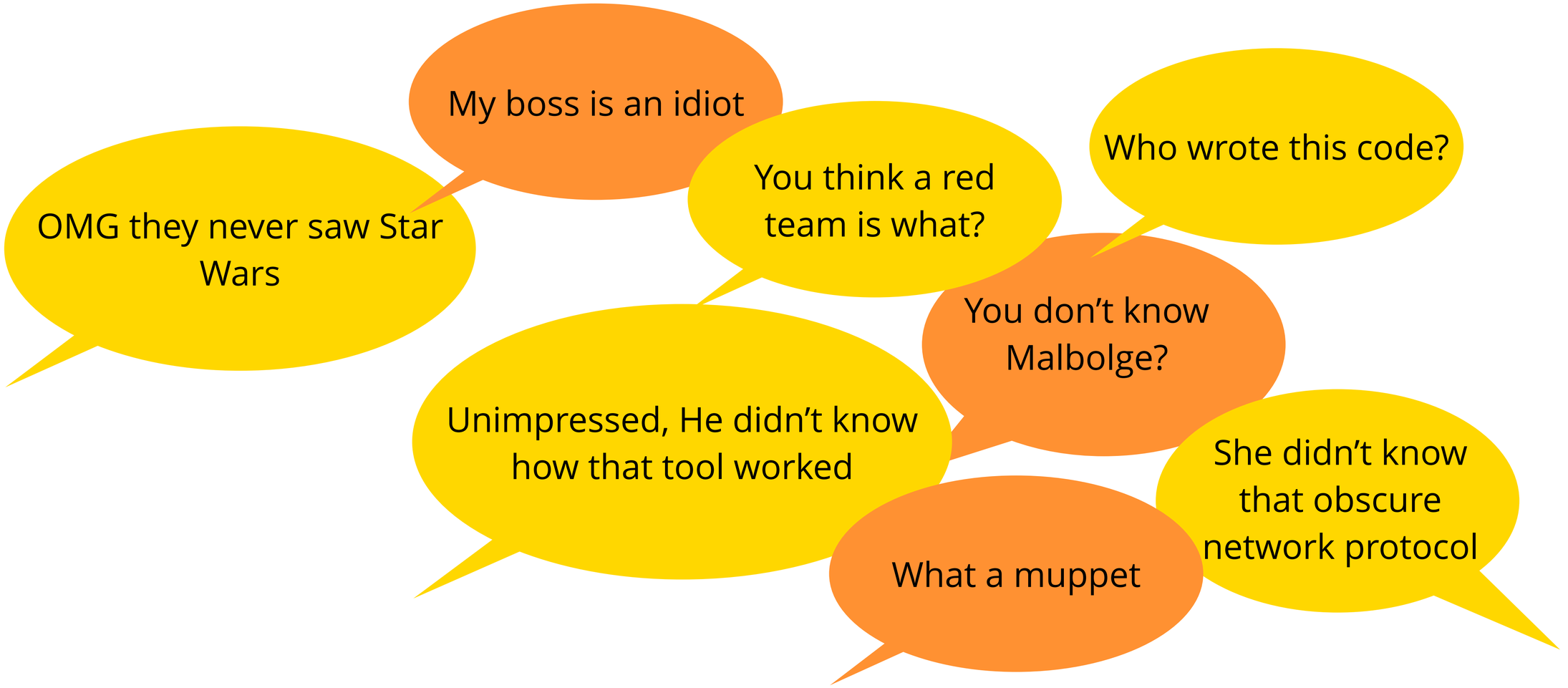
Workstations + mobiles + tablets+ servers + SaaS + “Cloud” + applications + people + their motivations + their lives + company strategy + economic factors + geography + the interaction of all these + pandemics + whatever else =

Your organization

*Never use the word “bespoke”...you know who you are.

Lesson 7: Everyone else doesn't suck

"Nobody's perfect....well, almost nobody" - Lex Luthor



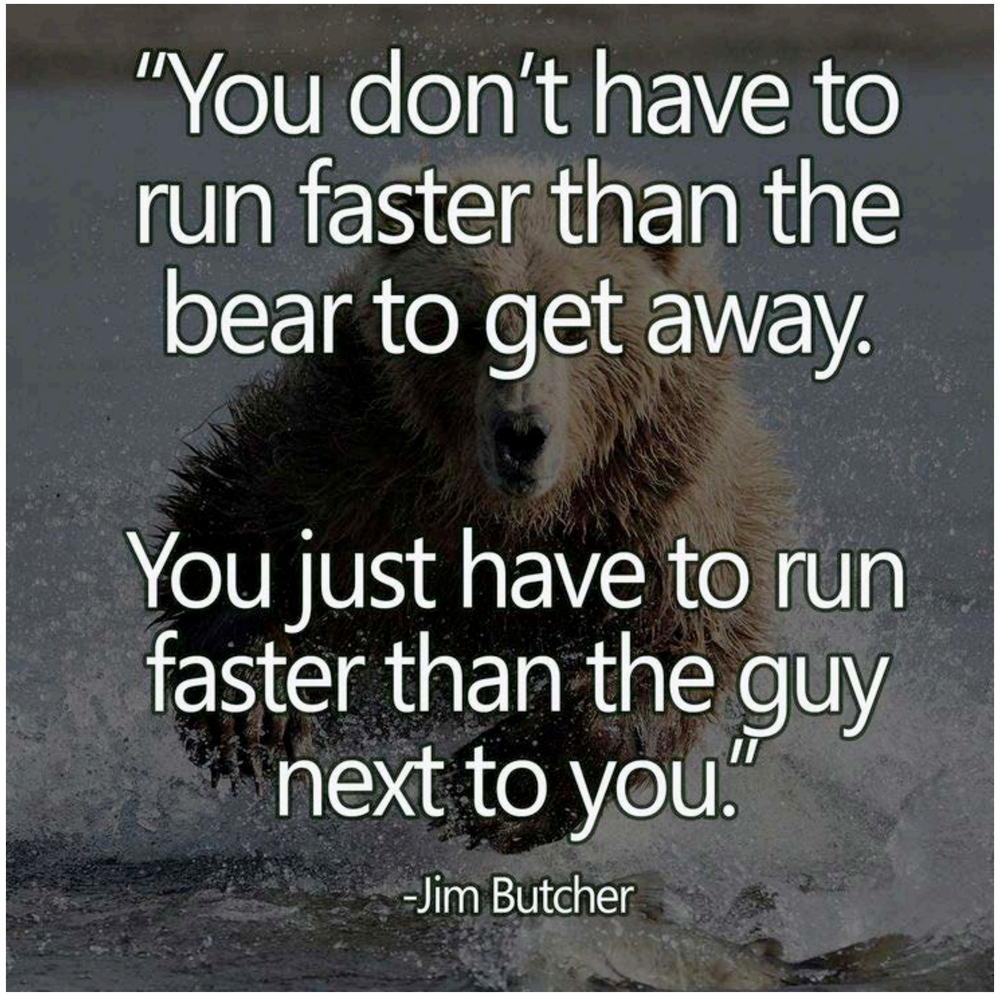
Lesson 8 : An unfortunate truth #1

Endless Hype

Pay to play

Crazy Investment

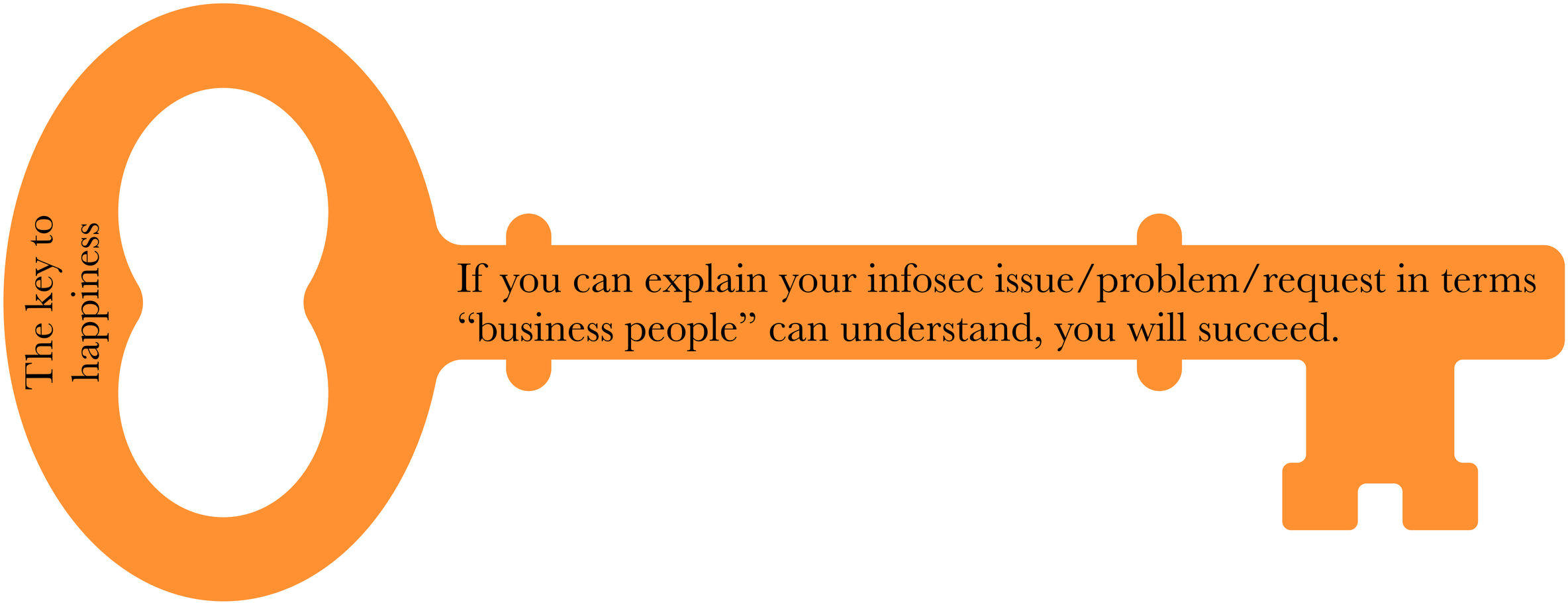
Lesson 9: An unfortunate truth #2



Extra Question: Does this relate to expenditure?

Lesson 10: Speak “business”

Context is king



Bonus Lesson

Beware of anyone who has a lot of certs.

Finally - Be yourself

Yes you need to pay your mortgage, buy cat food, take holidays, enjoy hobbies, and all that other stuff that needs money. However, do you need to “sell out”?

More and more evidence that actually, being honest in this game will get you where you want.

Senior management, co-workers, employees, are all suffering from infosec fatigue.

So maybe not doing everything the same way is the right course.

Thank you OWASP London

Mark.Stamford@occamsec.com

www.occamsec.com