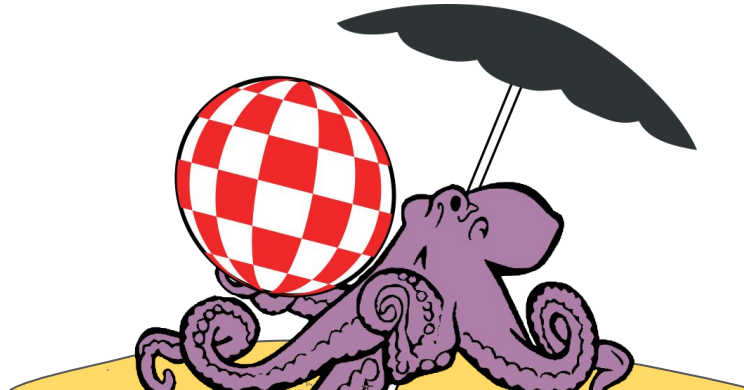
*NEW SLIDES

INFOSEC & FAILURES

ANGE 👼 ĄŻ杏 ALBERTINI

HACK.LU - OCTOBER 2017



This talk is **not** about "funny" failures

...not about making fun of people *failing* to *understand* or *unable* to take measures.

That's patronizing at best, and often bullying.

http://gunshowcomic.com/648

Same old song.

See? I told you!

I me mine.

They suck.

Infosec is typically about winning

A series of "Success stories" to impress/motivate you.

They present their wins, but you don't see their numerous failures.

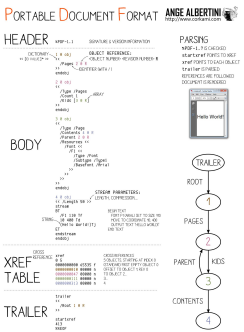
Stars **waste** their energy to become big and create hot air, *black holes* naturally attract others.

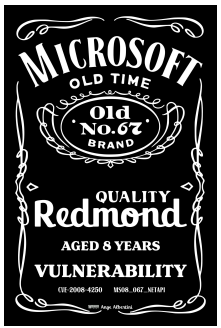
There's a lot to learn from others' failures

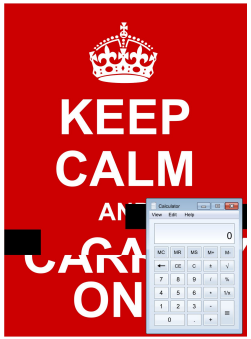
- tune down your impostor syndrome.
- the grass is not that green on the other side...

THE PRESENTER

- INTERESTED IN INFOSEC SINCE 1989
- VIDEO GAMES PRESERVATION SINCE 1999
- DRAWING SINCE 2012







comme endommagés dans la table d'allocation des fichiers. Par chance, il n'attaque que les IBM PC-XT. Pour s'en débarrasser, il faut rétablir les pistes de démarrage dans leur état d'origine. Avec un éditeur d'octets du type PC-Tools, vérifiez la présence des octets 33 C0 dans les zones 30 et 31 du secteur d'amorçage du disque dur ; s'ils sont bien présents, mieux vaut exécuter la commande SYS depuis une disquette Système saine ; à la fin de la première table d'allocation des fichiers du disque dur, remplacez les trois derniers octets (FF 7F FF) par FF 0F 00. Puis localisez le code du virus lui-même, qui commence par FF 06 F3 7D 8B 1E, et remplacez-le (ainsi que tous les octets qui suivent, jusqu'à 55 AA) par F6 si le formatage est dû à la commande FORMAT du système, ou par 00 s'il provient de PC-Tools. Si l'opération vous semble trop com-

http://fr.1001mags.com/parution/svm/numero-66-novembre-1989/page-146-147-texte-integral

INSTRUCTIONS TO **MANUALLY** REMOVE A BOOT SECTOR VIRUS WITH A **HEX EDITOR** IN A FRENCH MAGAZINE IN **1989**.

ALL OPINIONS EXPRESSED DURING THIS PRESENTATION ARE MINE AND NOT OF MY EMPLOYER(S), PRESENT OR PAST.

As you probably just noticed,

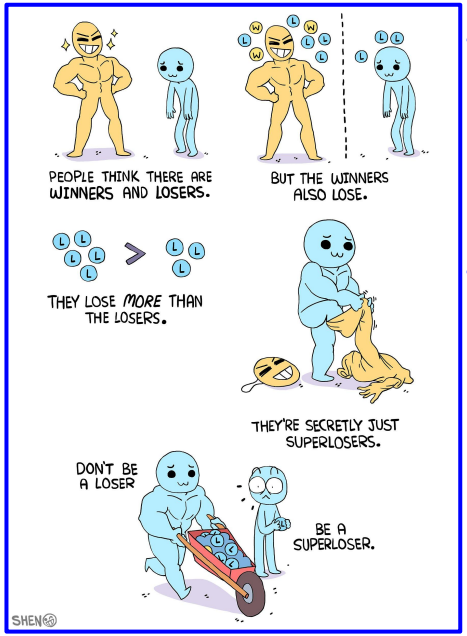
I'm not a psychologist.

No complex concepts, no latin words.
I can't parse their format anyway.

*

THE TALK

- ANOTHER ENUMERATION OF <WORKED FOR ME>?
- I'VE BEEN ALREADY TOLD THAT I'M "SUCCESSFUL".
  BUT ACCORDING TO WHAT?



http://owlturd.com/post/166478439794

- BEHIND EACH OF MY "SUCCESSES", SO MANY FAILURES MY HEAD HURTS.
- THERE'S PLENTY OF STUFF I'D LIKE TO HAVE BEEN TOLD BEFORE.
  SO HERE THEY ARE - THEY MIGHT SOUND OBVIOUS, OR NOT.

This is a 2 part talk, about 2 kinds of failures...

Group / Personal

I keep seeing the same repeated recipe with the same baseless hope for change.

You can't find anything new if you keep trying the same way.

I've seen too many people burning out.

And many people don't understand the difficulties of infosec.

Group failure

What could we improve?

Infosec feels like an oral tradition.

To study a new topic, you have to jump
from talks to article to blog posts.
It looks ok, but nothing happens when a link dies.

Share differently?

Too many conferences.

Conferences -> paper -> 1 URL -> single point of failure?

Preserve knowledge

Just rely on the Internet Archive and VirusTotal ?
Knowledge preservation is about content preservation,
not file structure - actual PoC crafting

We can't even replay old exploits
and learn from them.
Retrogaming was weird/awesome
when it started, now it's mainstream.
How long before **RetroPwning** is a thing?

How long before we store a Vm snapshot - not just a PoC - per working exploit?

We can't even re-use our own knowledge.

Yet we blame others for 'not knowing' or not listening to us.
So many... conferences, talks, FUD, snake oil, buzzwords...
So much noise...

So many talks, then what...? Too much noise!

Up to each of us to sort everything ourselves...

(and it's tiring)

There's no trail of knowledge to follow.

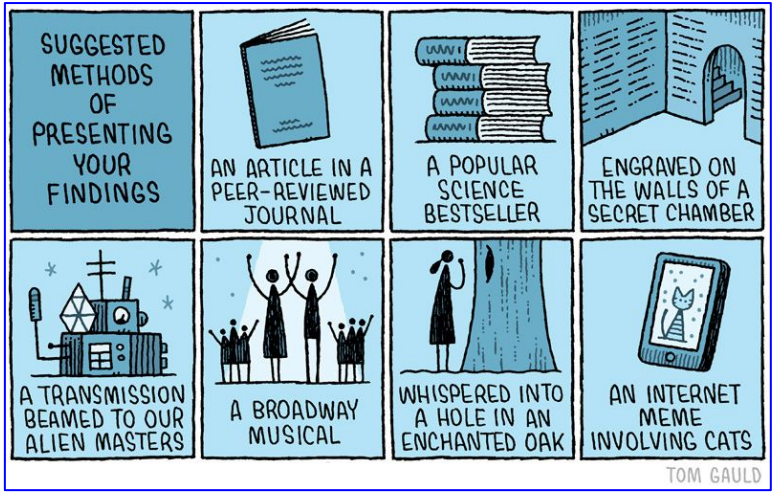
Too few experts. too few milestones to refer to.
And many broken links. Only Academia preserves.
Is the model of **free** slides bound to fail?

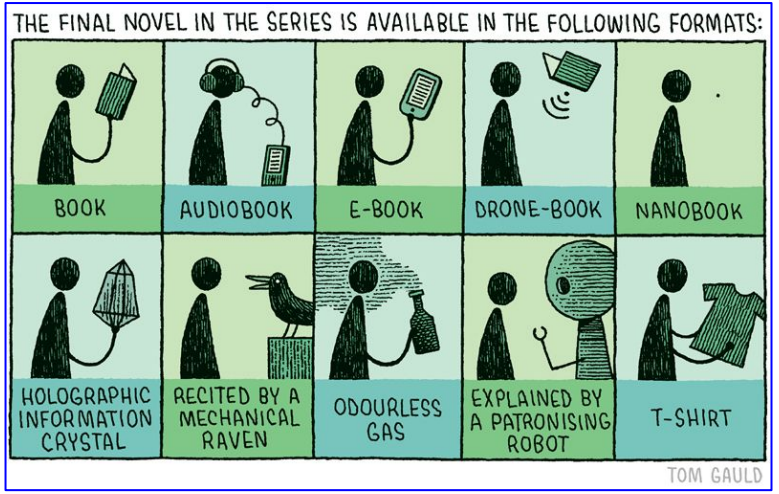
Books I'd buy.

Best of Hack.lu

Conference talks

Curse or blessing?





https://www.tomgauld.com/

PRESENTING

...IS OVERRATED!

IT'S NOT BECAUSE YOU CAN'T PRESENT THAT YOU CAN'T BE AMAZING.

(AND TOO OFTEN, A PRESENTATION IS **NOT** THE MOST USEFUL WAY TO SHARE YOUR FINDINGS)

PRESENTING IS FULL OF **ARBITRARY** STANDARDS

- "5 IDEAS PER SLIDES. 1 MIN PER IDEA. 15 SECS BETWEEN SLIDES" -

WHICH CAN BE A HUGE WASTE OF ENERGY.

Worried about your talk?

You were selected! Ask how many talks were **rejected**!

You **know** your topic, and you even **improved** since you submitted!

Be honest, be yourself, use your style:

Infosec **needs** moar diversity.

Pre-talk anxiety

It's just normal!

It's just that you're **focused** on the important things.

It won't disappear with experience, you'll just get used to it.

It just helps you to tone down little disturbing things
- such as lack of sleep, hunger... - before your talk.

Speaking in front of a bigger crowd is *easier* !

Just be careful of Q&A!

The bigger the crowd, the more stupid the questions,

(shameless people can hide more easily)

=> Politely redirect them to /dev/null

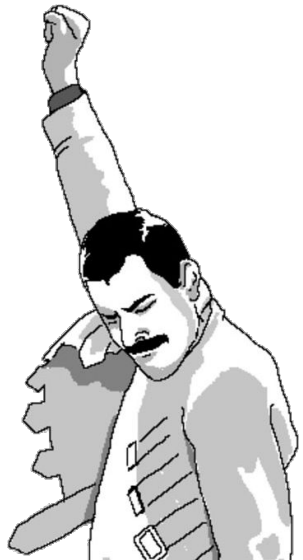
*

Imagine speaking in front of:
your employer, your parents [in laws], your banker,
the top 10 experts in the industry, and your worst enemy...
OMG my life is doomed!

Now imagine if they're all hidden in a huge crowd!
Pfew! Now they're much less likely to even reach the mike :)

Give yourself one last push before the talk

A shot of non-fuzzy alcohol,
Strike a victory pose,
your favorite music - YMMV!
It could improve your mood,
and consequently the whole talk.



More efficient than your next talk?

- Gather materials.
- Write notes.
- Prettify (optional)
- Share / sell

You can even do it
for someone else's content. =>

https://archive.org/details/4amthology

Infosec jumping the shark

https://twitter.com/MalwareTechBlog/status/920017904359186432

MalwareTech
@MalwareTechBlog

Follow

My favorite branded bug is still that BadLock one where the dude spent weeks hyping up a useless bug he found in his own code.

1:05 PM - 16 Oct 2017

Not enough responsibility?

Laws to back your claims?

Branded vulnerability? Crappy specs? Snake oil?
We know they're wrong,
But the culprits are still at large!

The Infosec crash is coming.

Like the video game crash of 1983?

Too much noise and hype

=> loss of trust/interest

Short-sighted goals are addictive.

Wait for measurable badness, fix, show impact.
Prevent an entire attack class... no measurable impact.
Guess which ones make your shareholders happy?

Short-sighted goals are here to stay.

Even breaches don't make so much financial impact.
Nothing will change until a breakpoint hits.
Insurances will eventually make a difference?
(they associate money with restrictions)

We're just at the start of a cycle...

Computer infosec is still very new.

I'm just trying to be realist,

but please prove me wrong :D

Personal failure

Nothing matters if
You're broken inside.

You are the most important person in infosec.

Because nothing will matter anymore if you're broken/burnt out.

Infosec makes it easy to burn out.

Bullsh*t bingo, Snake oil, drama...
It's seen as a gold mine by many opportunists.

If you're fine

people often look happy right before taking action:
they have already taken their decision,
so they feel "relieved".

LISTEN!

Since broken people

can't easily speak anymore.

If you're broken

Fix yourself...

...and then you can help and fix others later.

My most important advice

Infosec is about failure.

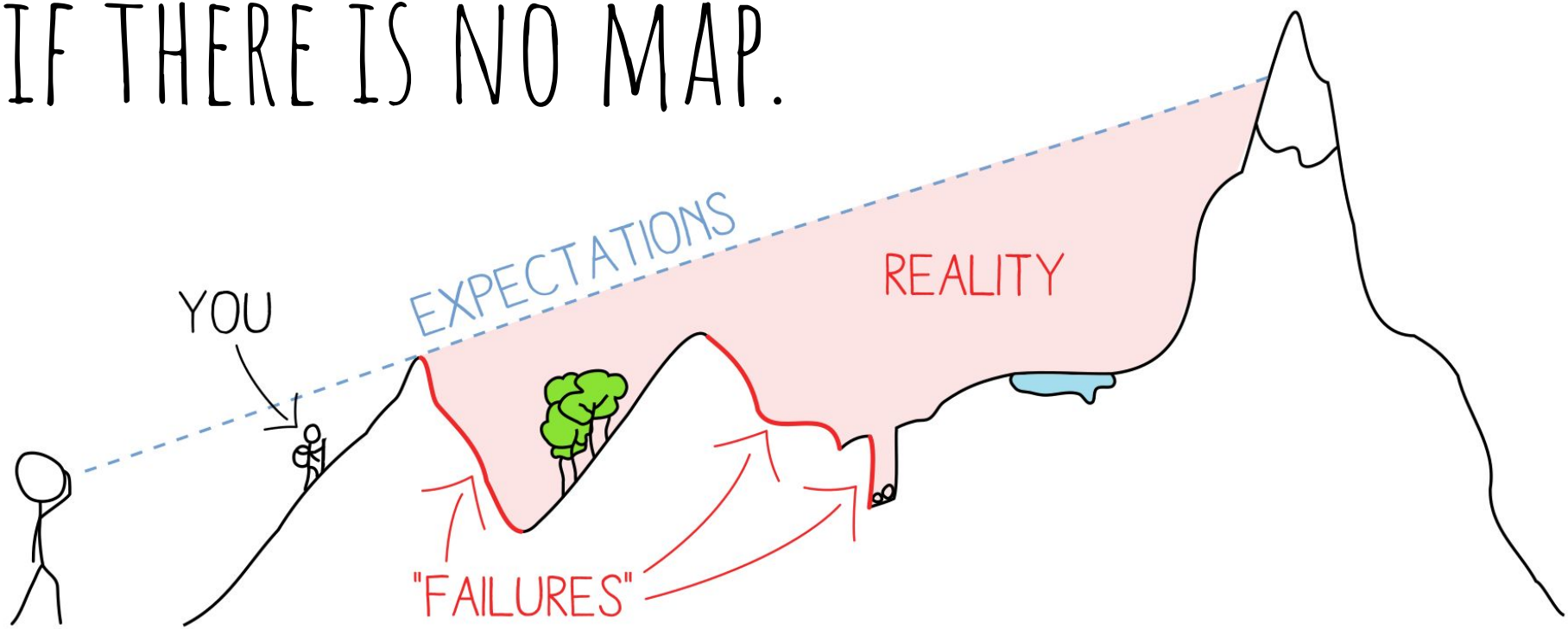
Accepting, embracing, avoiding...

It doesn't mean we **want** to fail!

But we need to **accept** the state of failure.

The knowledge will come. The more the better.

You can't know the path if there is no map.

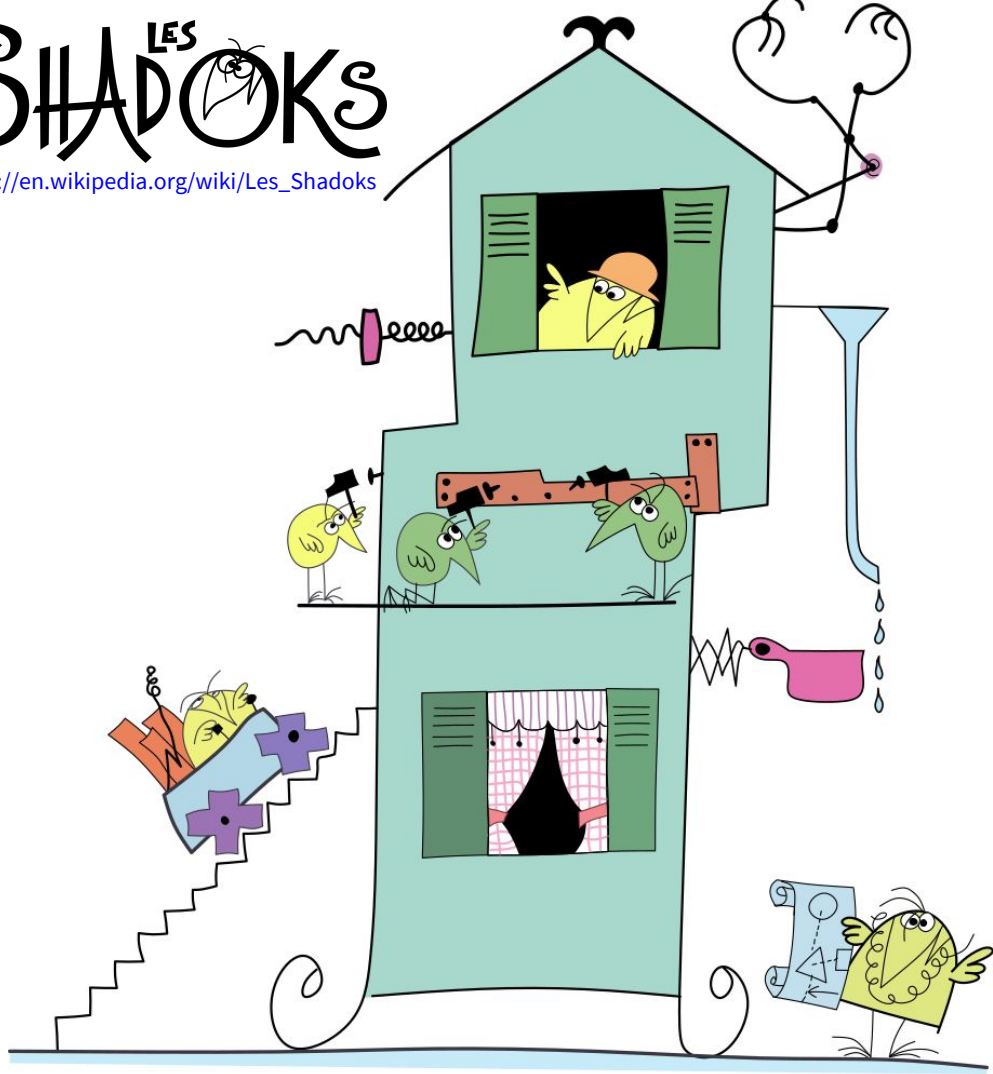


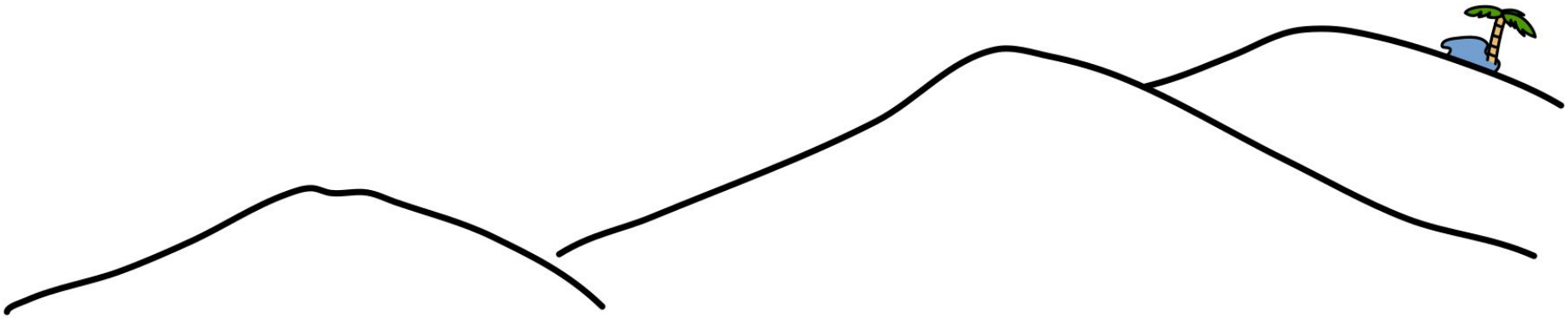
Les Shadoks

https://en.wikipedia.org/wiki/Les_Shadoks

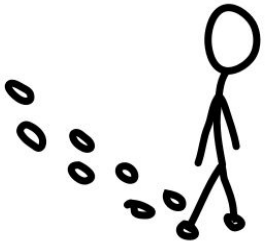
The Shadoks mentality:
1 chance in a million?
Fail 999,999 times ASAP!

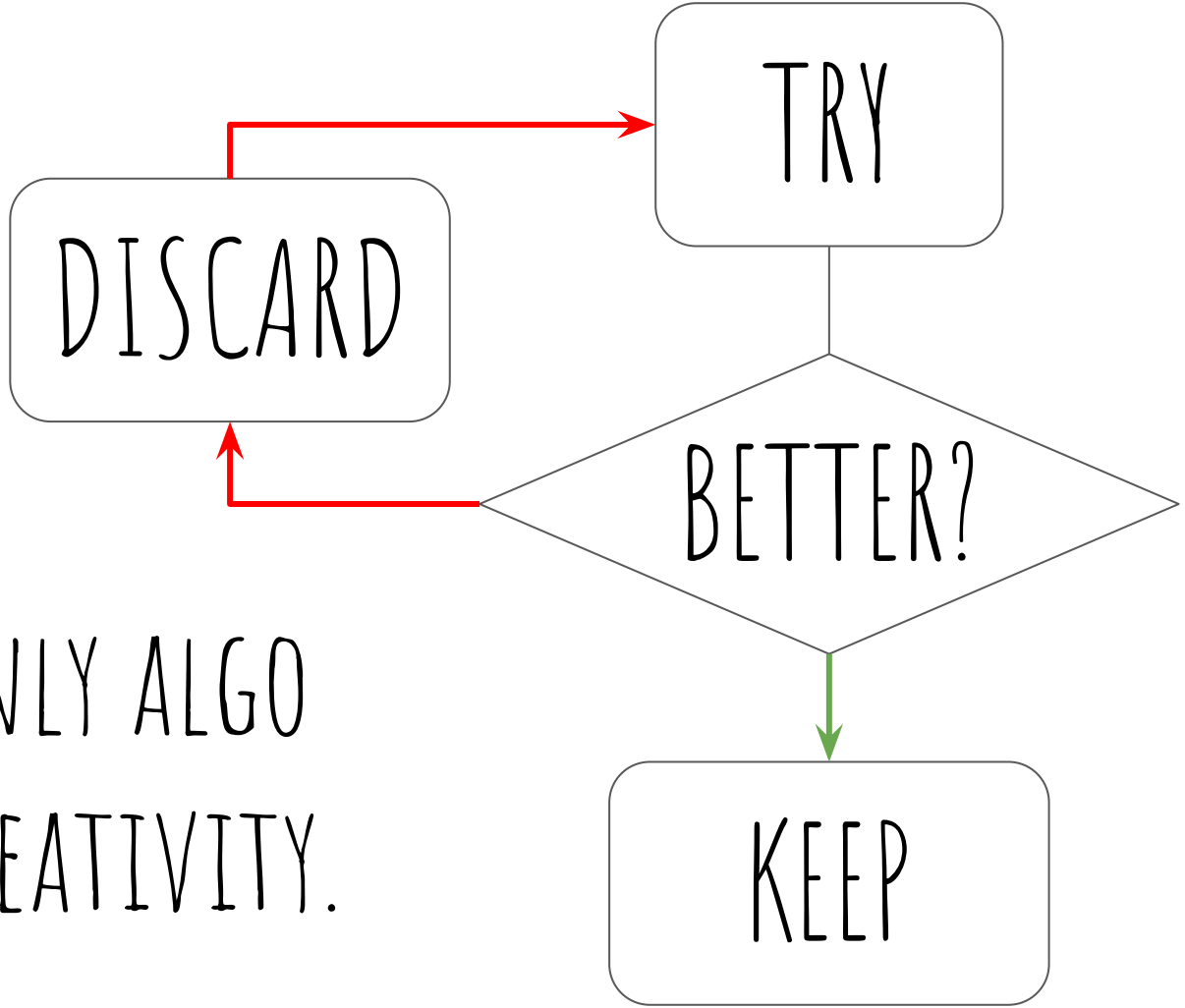
My motto:
let's fail! And learn why!





A single success is a long line of failures.





My only algo for creativity.

It's ok to...

- Have no idea what do to next
- To have taken the "wrong" path
- To have taken "too much" time

Loosing hope?

Can't beat the stage boss?
Get more XP in side quests!

Find yourself a sub-quest:

- to keep the engine running.
- to bring extra knowledge, in a playful way.

Letting the dough rest is not a cooking failure.
Keep that fidget spinning around your fingers.

Which one is the best?

PS: I have 2 I.S. feeding each other (for reversing and for drawing).

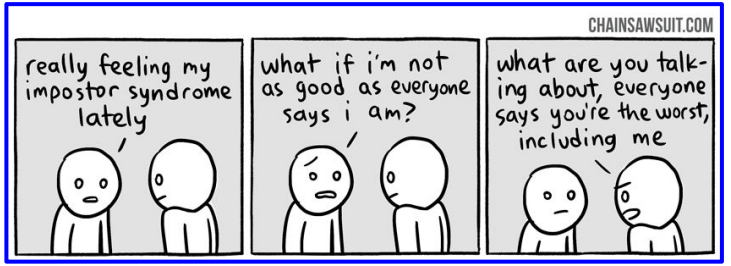
How good you think you are

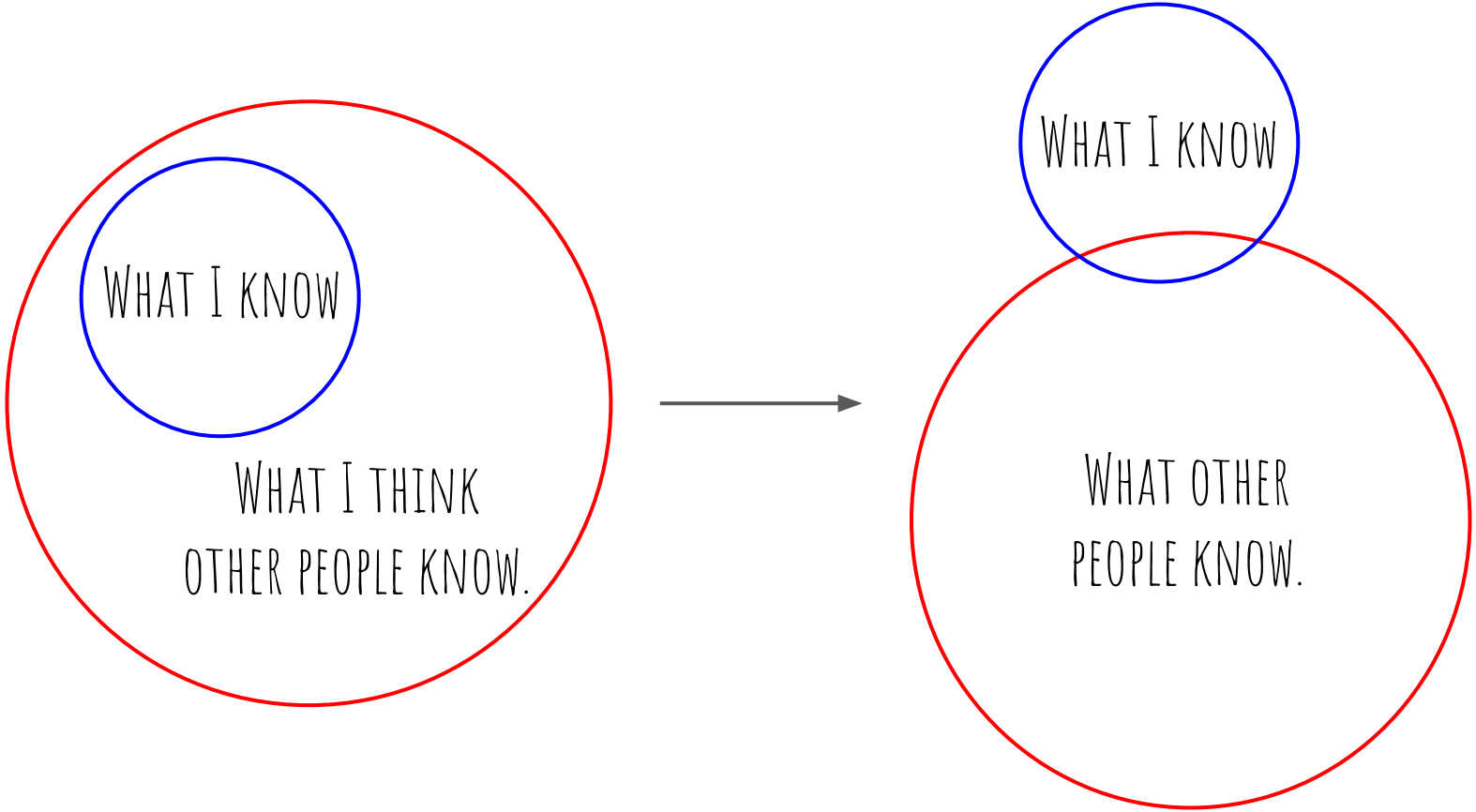
Dunning-Kruger effect (shameless ignorant)

Impostor syndrome (conscientious expert)

How good you are

http://chainsawsuit.com/comic/archive/2014/09/02/impostors-revealed/




What I know
What I think
other people know.
What I know
What other
people know.

All you need is the right challenge.

Turn your daily routine in fun challenges.

InfoSec can be veeeery boring...

Spare energy

What doesn't kill you make you stronger:

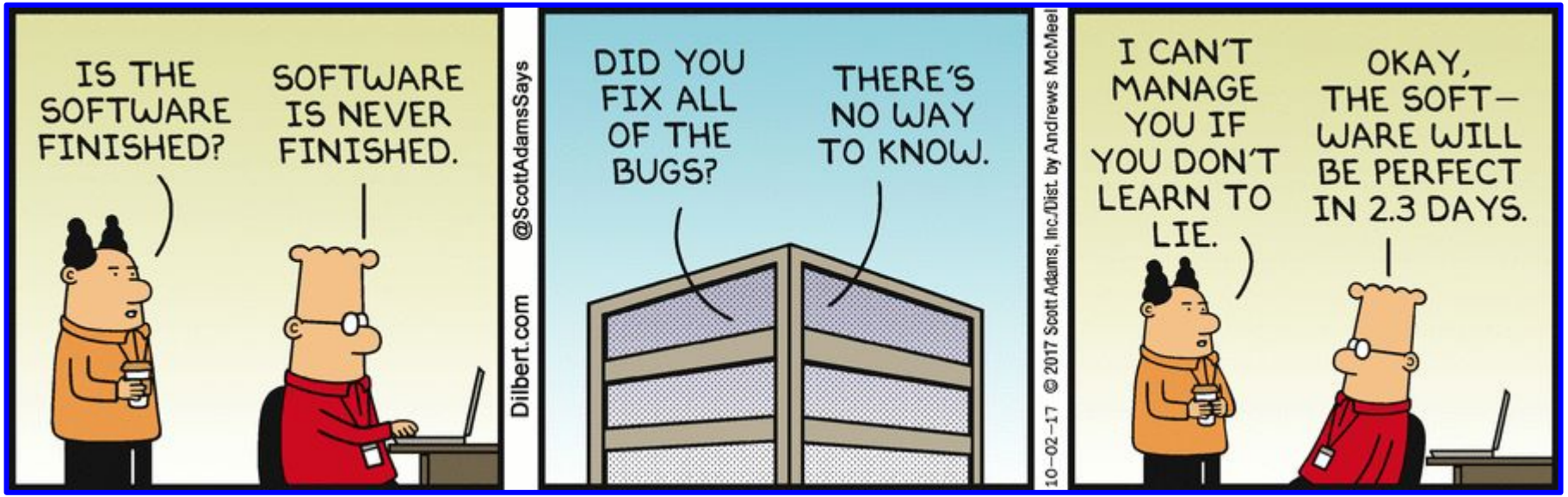
choose your archenemy wisely.

Don't spend too much energy with the minions.

Blame the game, not the players!

Be careful of power dissipators!

http://dilbert.com/strip/2017-10-02



Forgive

You'll spare some energy for yourself.

Try walking in their shoes before blaming.

Do not forget

That's nitro for your willpower.

TBH you **don't** need an archenemy.

Finding a mentor / soulmate
Can change your world.

anyway, just ignore the players.

Most of them don't deserve to be your enemy.

Diversity is good!

For your brain, for your skills.

People outside your speciality or even infosec can really make a difference in your work/life.

Go and speak to people. Outside your team, outside your comfort zone.

Out of fuel?

Take a break!

(I know, it's *hard* sometimes)

Your friend can't take a break?

Insist! "Force them"!

Break their phone! Kidnap them (j/k)

Ultimately...

you don't owe Infosec anything!

Feel free to leave

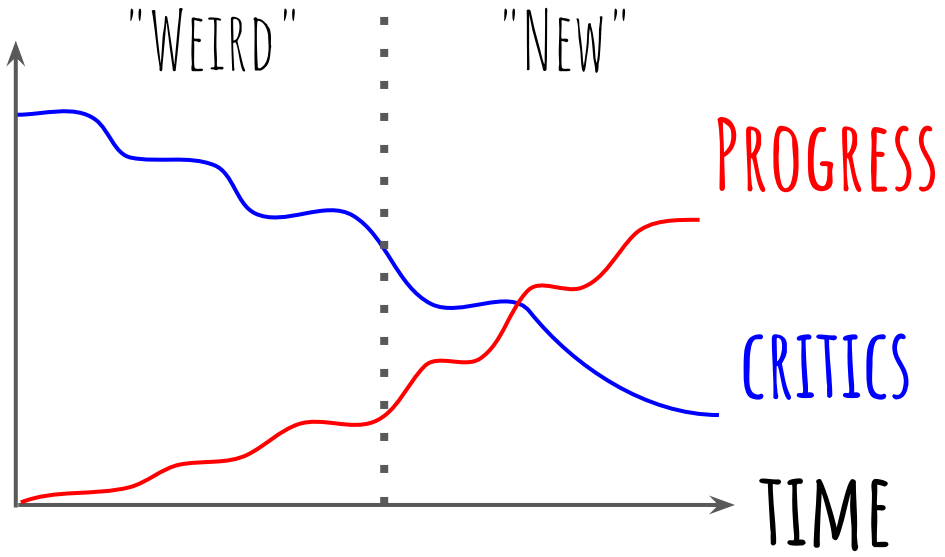
(some awesome people in Infosec are "just" hobbyists)

Come back if you wish, as you are.

Others can't always share your perspective.

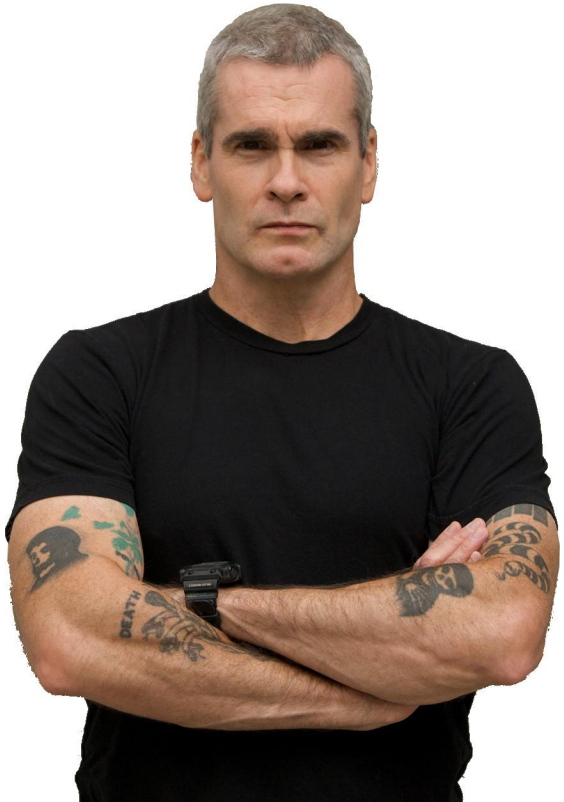
No, not even your closest friends.

Follow your convictions - and try!



if I'd listened everything that they said to me,
I wouldn't be here!
and if I took the time to bleed
from all the tiny little arrows shot my way,
I wouldn't be here!
the ones who don't do anything
are always the ones who try to put you down
and you could spend your entire life walking around
in the nowhere land of self doubt

Henry Rollins - Shine



Can't make big plans?

Just be a lemming!

just one. single. tiny. step at a time.

repeat

There's no useless step.

A tiny weird gear **now**
could be the missing piece
in a whole engine **later**.

Can't get motivated?
Set a deadline w/ a 3rd party

Just make a tiny bet with a friend,
And imagine their grin if you fail.

Deadline as a Service ? :)

It has to start somewhere

It has to start sometime

What better place than here,

What better time than now?

RATM - Guerilla Radio

If we don't take action now,

We settle for nothing later

RATM - Settle for Nothing

Cherish your little flame

Keep some *daily* time for yourself
To do your own *personal* stuff.
Maybe do it right at the start of the day!

Whatever rocks your boat, really!

Your shadow is for Plato's cave - keep the flame for yourself!

You can't take care of anything/-one
if you can't **take care of yourself** first!

And your body too,
there's no health credit!

You're not ugly,
You're just
not your type.

You were born with a specific body,
but your brain later decided
to prefer a different kind.

Appreciate your body,
it's your best supporter.

*

Diploms?
Where we're going,
We don't need diploms.

Data is addictive:

we can't help judging arbitrarily.

=> Drop some tables

and give people more air.

Linux/Windows, IDA/Radare, Vi/Emacs, Tab/Spaces, Intel/At&t, Certifications...

Don't worship

Everyone makes mistake,

(and everyone eventually gets replaced)

so anyone could be proved wrong.

Listen, but also try.

Best answer to feedback: "what did you try?"

Need ideas?

You probably have great ideas - There's no jungle in Finland ;)

Disconnect: all devices off, out of reach, out of view.

Isolate: noise cancelling, background noise, shower, bar...

Pen & paper: to not forget without being disturbed.

Or a laptop with a single open editor window at best.

Speak out ~~loud~~: put your brain at rest.

10 mins of purge your daily misery, 10 mins of cold boot.

Uninteresting people makes excellent whitenoise generator :P

Keeping ideas

They go away too fast, really!
Keep a notebook with you, next to your bed.
And yes, wake up at night to write them down.
You'll be grateful the next day.

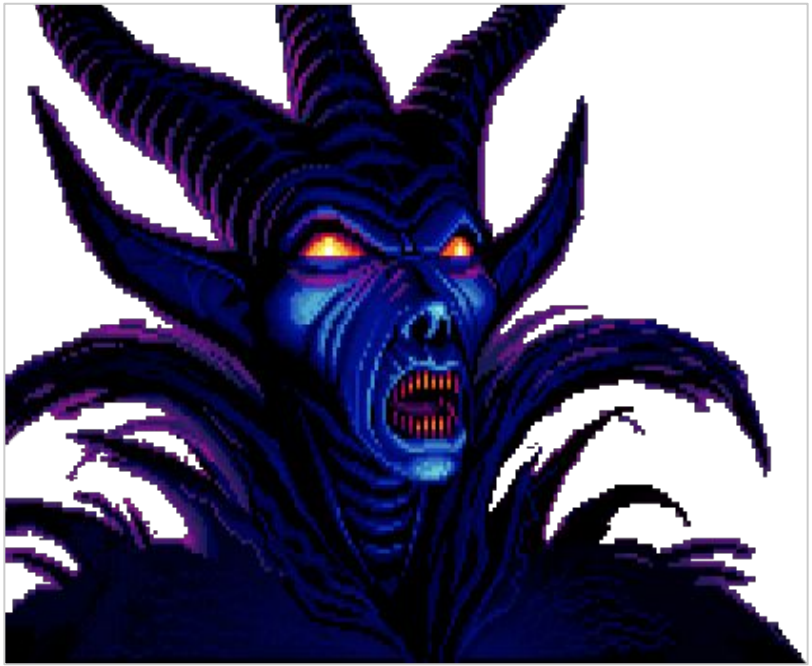
If you don't even try,
your idea is worth **nothing**.

If you don't try your own idea,
you can't convince anyone else to.

Your ideas are born in their most favorable ecosystem: you.

If you feel out of place
in this world,
then you were born
to create your own.

Death (can't be more gloomy, can we?)



Don't take it like this...

Death is just the last **action** in your own game. What will you do before?

BPX ExitProcess. Run. Break.
What's on your memory dump?

Conclusion

(Wow, that was gloomy)

Don't take all this too seriously, I'm only sharing opinions!

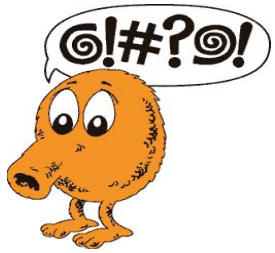
I even fail at writing proper conclusions.

Don't mind me, I'm just an impostor ;)

Fixing the world's systems
starts by fixing infosec.

Fixing infosec starts
by taking care of yourself.

I wish you happy wins...
...and many constructive fails ;)



Reminder:

It's about using your energy wisely.

Not an excuse to be a @!#?@!:

A @!#?@! stays a @!#?@!.

"Cry me a river" ?*

No privilege prevents your brain to mess you up.

(color, religion, gender, orientation, health, wealth...)

Yes, I probably have it easy.

Thanks!

Feedback?

Acknowledgments:

NewSoft, Gynvael, Doegox, Halvar

Joachim, Bruno, Claudio, Barbie, Paul.

ANGE ALBERTINI

reverse engineering

VISUAL DOCUMENTATIONS

@angealbertini

ange@corkami.com

http://www.corkami.com