Education & communication

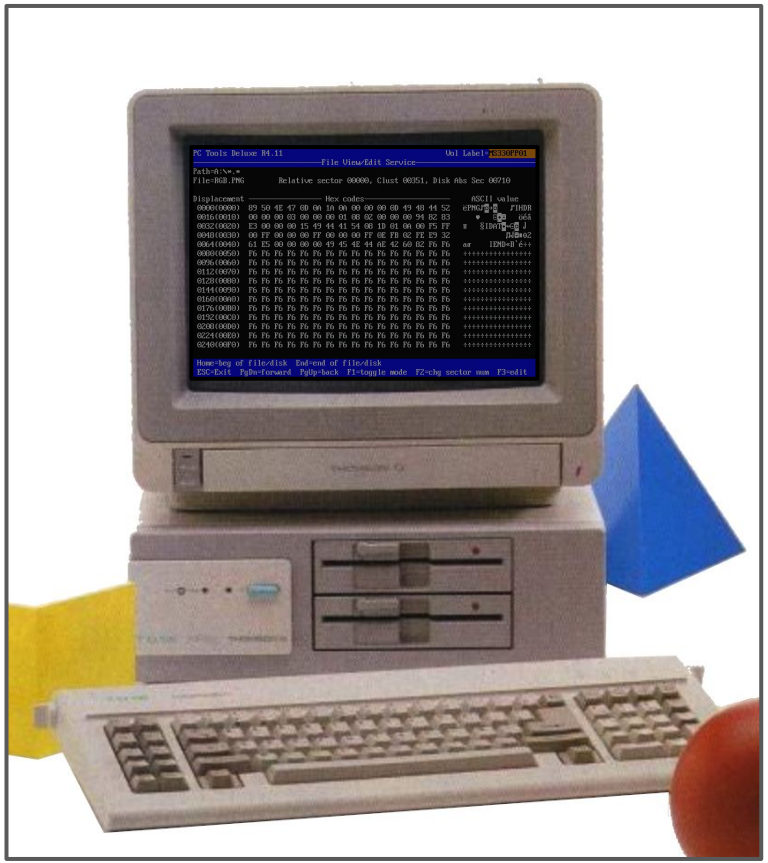
Ange Albertini

Hack.lu
October 2018

Ange Albertini

Interested in InfoSec since ~1989

Currently Security Engineer at Google.



All opinions expressed during this presentation are mine and not of my employer(s), present or past.

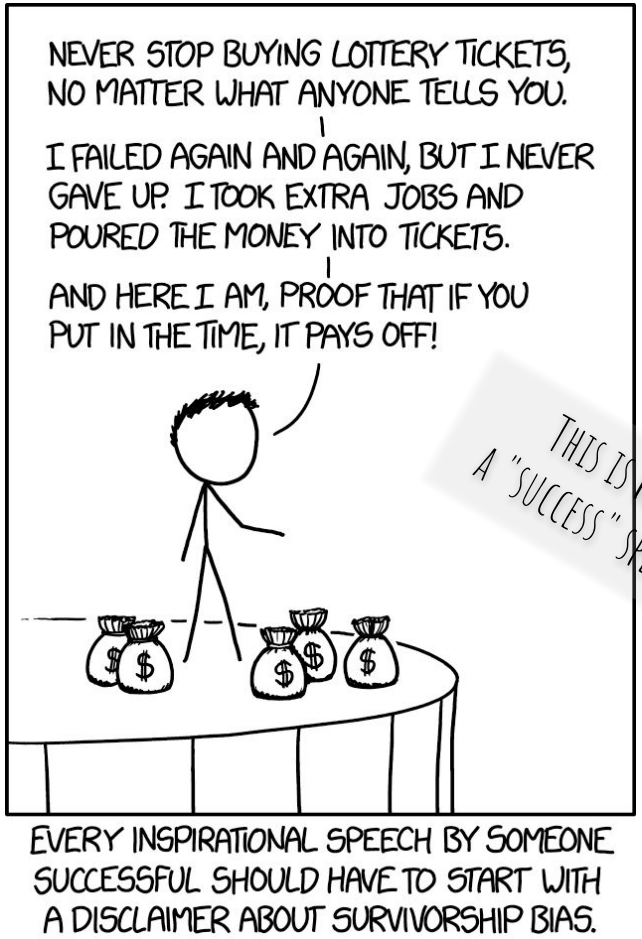
Episode III

LAST EPISODE OF THIS KEYNOTE TRILOGY

This talk is **not** about showing off my *success*.

Focusing on the basics.
Not necessary limited to Infosec.
Totally experimental. Unpopular opinions?
I'm obviously biased. I'm here to share & learn.

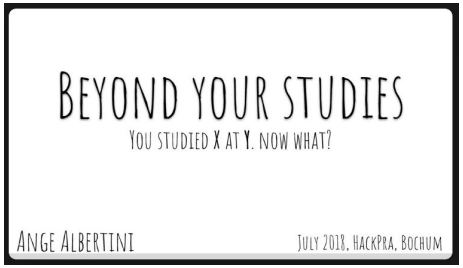
Survivorship bias https://xkcd.com/1827/



THIS IS NOT A "SUCCESS" SPEECH.

Topics of the previous episodes

1. your future (as a student)
2. Yourself
3. Your surroundings (this talk)



Beyond your studies
https://speakerdeck.com/ange/beyond-your-studies

Infosec & failures
https://speakerdeck.com/ange/infosec-and-failures

This talk is...

Dedicated to those who
blame, humiliate or belittle,
and pretend they're superior or professional.

Blue Chair ep 405: Basically.

Imagine a life where Everything is secure

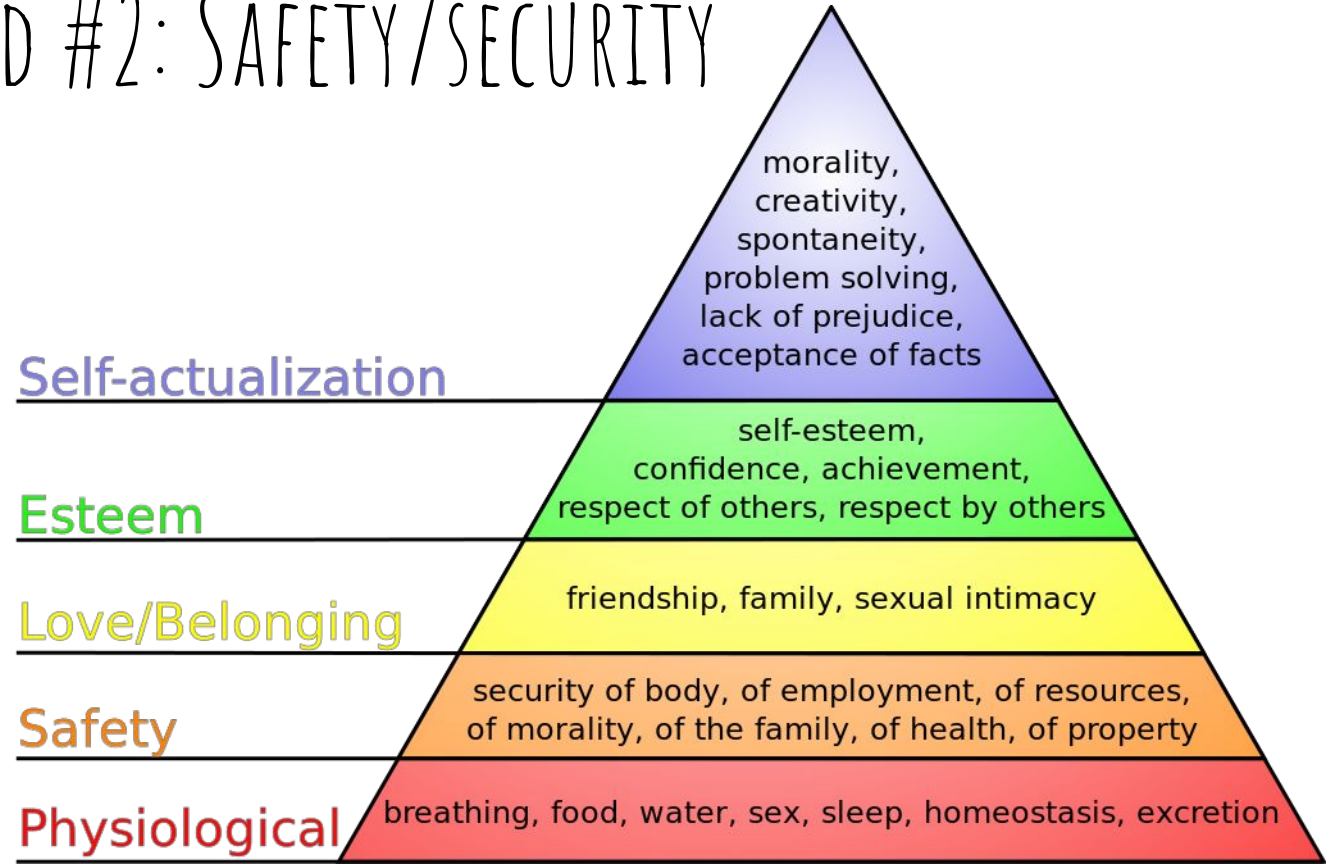
Nothing would work, right?

Does your baker read Phrack or explore arXiv?

Our daily life is bound to computers

We all carry a powerful computer with us now:
computers are not reserved to experts anymore.

Essential need #2: Safety/security



https://en.wikipedia.org/wiki/Maslow%27s_hierarchy_of_needs

Unpopular opinion

Infosec is a life requirement

for **everyone**.

Experts are a need for non-experts.

That's why they have a job ;)

We need to share our expertise

We're the 1%

whether we like it or not.

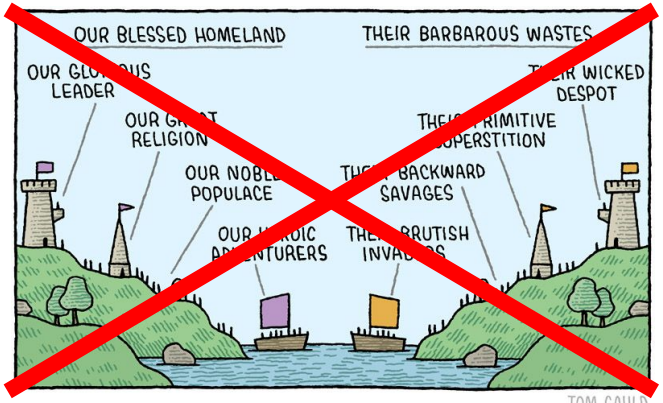
We're on the same boat

It's not **US VS THEM** : There's no ivory tower.

They screw up -> our whole security lowers.

We make understand -> the overall security and awareness will improve.

</slightly optimistic>



https://twitter.com/tomgauld/status/571994690289061888

I know what you're thinking...

Who cares!?

Well then, let those *ignorants* spread their own knowledge.

Story time

Remember...

Kids ≃ Users

End-users
Devs
Hierarchy

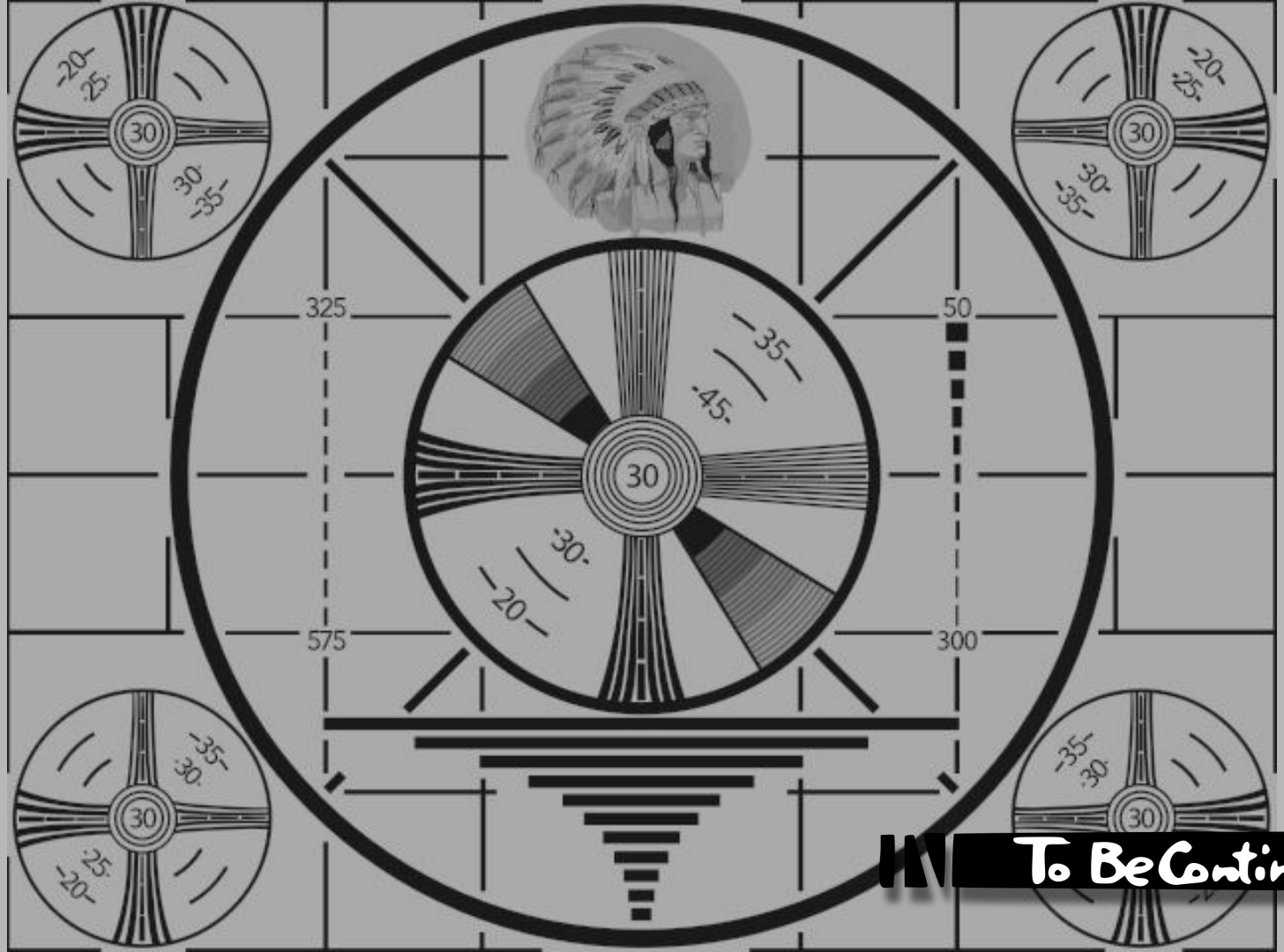
They're not expert. They can be knowledgeable.
Hard to be interested. Easily bored or intimidated.

If you don't care about 'idiots',
maybe you'll care about a mini-you?

Unpopular opinion

Education & communication is a part of our job.

We're experts in what other needs.
We have some responsibility.
And it also helps to convince our boss!


20
25
30
30
35
325
50
35
45
30
30
20
575
300
35
30
25
20
To Be Continued

BTW...

What's a hacker?

Everybody has their own definition maybe?
(pride blinds - no gatekeeping please...)

Black Hoodie :P

How do you recognize hackers?

Hackers care about their expertise, not their appearance.
The next person you're talking to may be as good as you are.
What's important is inside.

curiosity
+ activity
+ creativity

---

hacking

What is "hacking"?

First, a state of mind (curiosity) then comes expertise.

"...My crime is that of curiosity...."

the Mentor

Hacker manifesto
http://phrack.org/issues/7/3.html

Unpopular opinion

We're **all** born hackers.

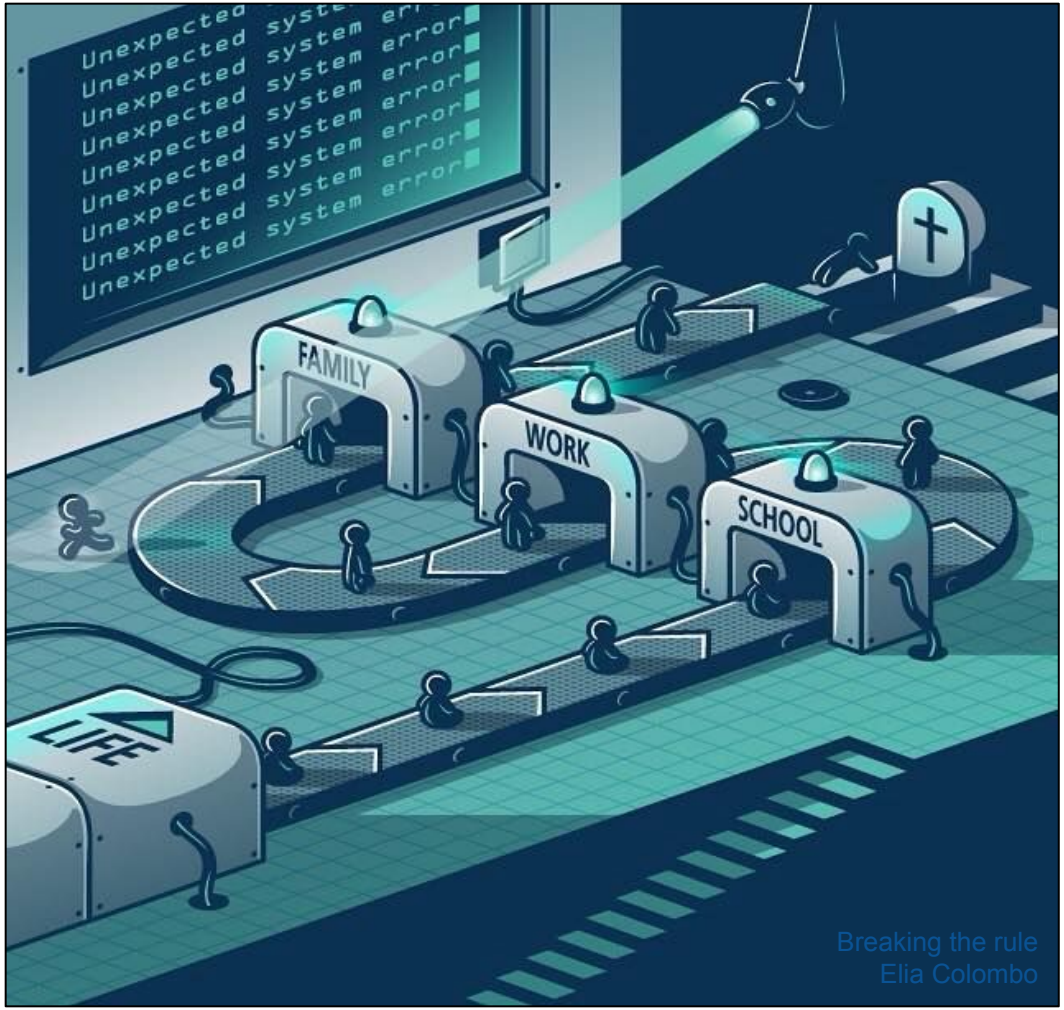
(Including "non-hackers")

We're **naturally** curious and experimenting.

"The floor is lava"

Our only instruction at birth is: put in mouth, suck on it.

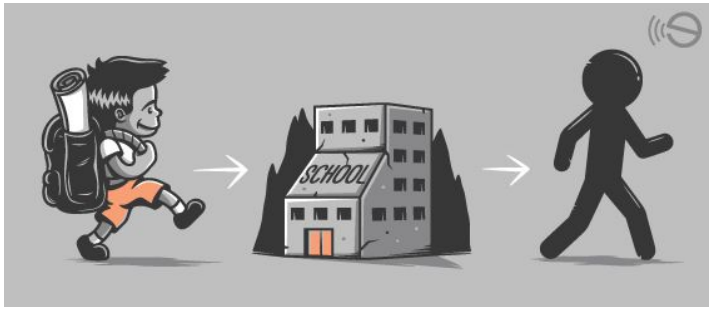
What happens later then?



Breaking the rule
Elia Colombo

We're sorted in categories.

We're formatted.



Classrooms are the worst way to learn?

Enforcing rules arbitrarily. you fail because you didn't answer the expected way.

Listening. Staying still. boring, no emotional connection.

Ignoring the brain's 'availability' windows.

Actual goal: learning social rules w/ some knowledge spamming. Doesn't work with everyone.

Worship the best. Shame the worst. game the system, hype.

-> as adults in the same boat, we need to move beyond that model.

Story time

Standardized education gives a system to game.

Rewards & punishments depend on following guidelines.

A 'little' sacrifice of everyone's creativity
so that life is easier for everyone else.

Story time

Standardized education *tends to* squash this curiosity.

They don't "give up",
they adapt to their environment!

It's just natural!

"Learn the rules so that you can break them later!", they say.

Our lives follow models: it's just normal!

You expect the same money to work the same way in shops.
All bakeries have the same rule.

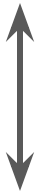
Even hackers share 99% of the DNA of monkeys.
Our differences are minimal.

Many "users" still have that curiosity.

Just not for computer and security.
(thankfully!)

Story time

Standardized education defines the norm. END-USER



Security cares about the exception. EXPERT

(this is not specific to InfoSec)

"They're no hacker: I've never heard of them."

Skills == fame ? Not really

Giving talks < attending cons < real name < social media < online presence.
If you have nothing to prove, you have no time to waste with fame.

Some people just use their hacker creativity on different things
and couldn't care less about CVEs and BlackHat.

There's no "idiot"

Or at least, not all of them ;)

I know stuff you don't. So what?
Not knowing is not a crime, nor a mistake.

I'm totally clueless about many things that are obvious to each of you.

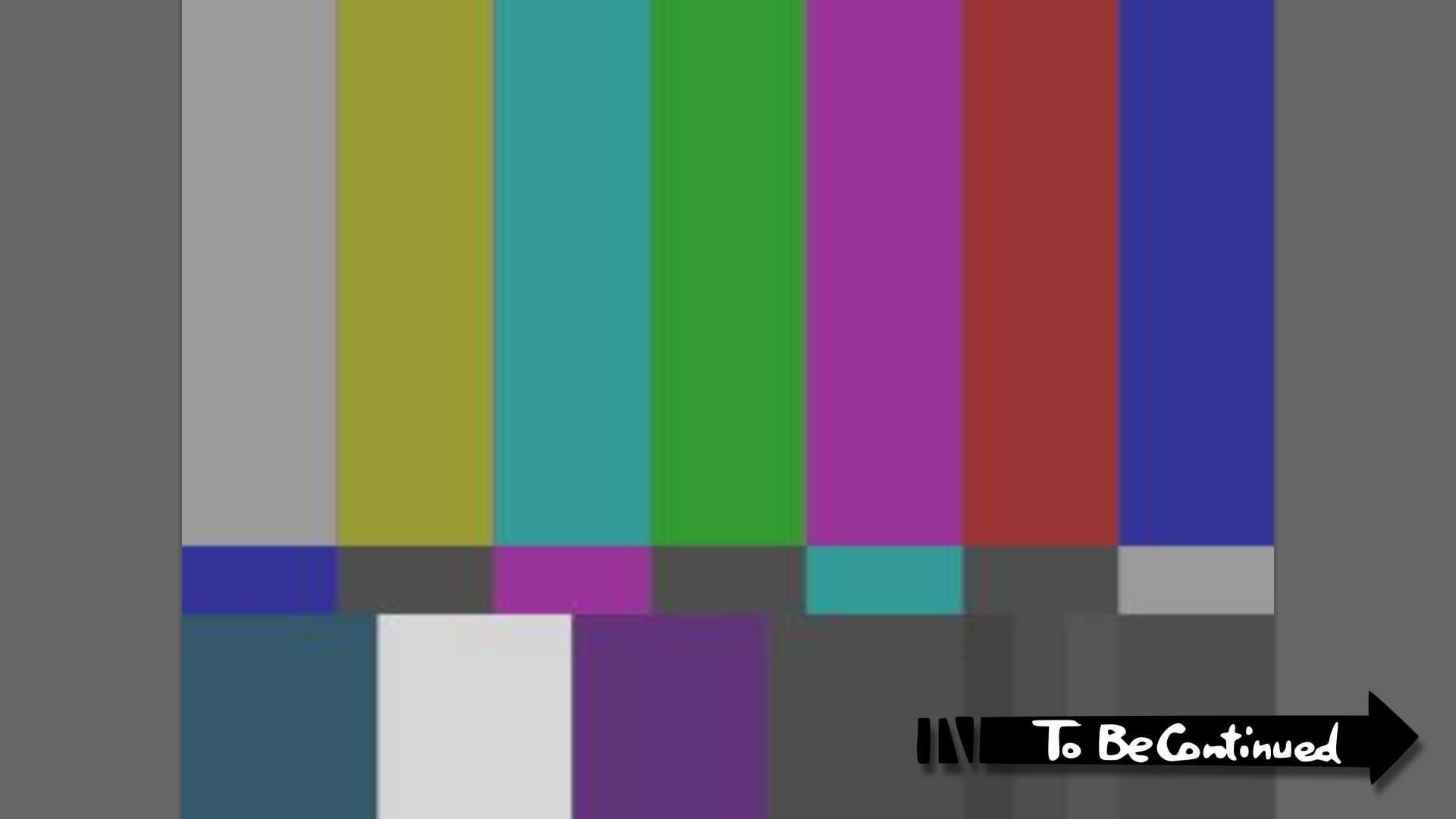
Belittling only shows you're arrogant, immature or impatient.

Unpopular opinion

Hackers are not "superior".

We have different passions like many other people.
It's time to leave that ivory tower.

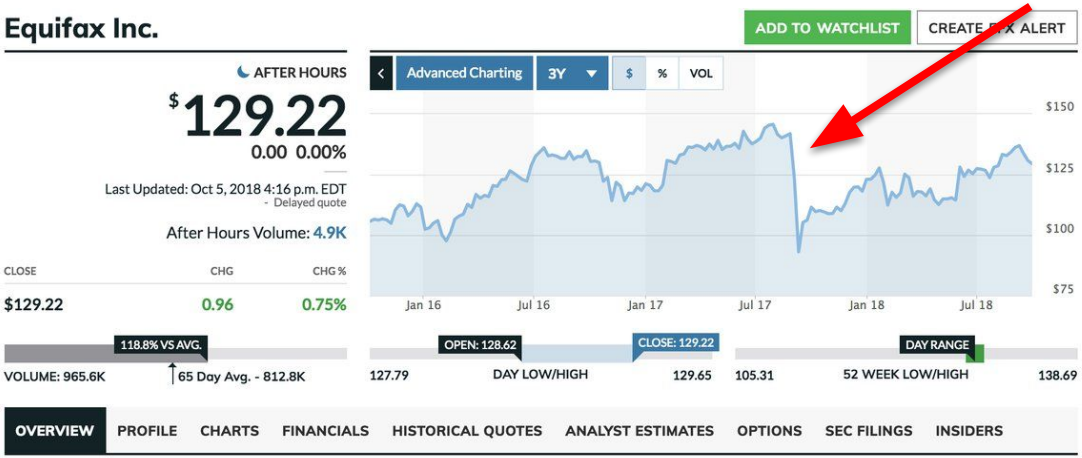
By design, [Information] Security is
at the opposite of standardized education.


To Be Continued

How old is InfoSec?

It's starting to be taken seriously.

We don't need to prove that hacks hurts or kill.



Webhost hack wipes out data for 100,000 sites

Vaserv suspects zero-day virtualization vuln

By Dan Goodin 8 Jun 2009 at 20:02 58 SHARE ▼

A large internet service provider said data for as many as 100,000 websites was destroyed by attackers who targeted a zero-day vulnerability in a widely-used virtualization application.

https://www.theregister.co.uk/2009/06/08/webhost_attack/

LxLabs boss found hanged after vuln wipes websites

Shocking development in VAserv megahack affair

By John Leyden 9 Jun 2009 at 08:38 6 SHARE ▼

The boss of Indian software firm LxLabs was found dead in a suspected suicide on Monday.

Reports of the death of K T Ligesh, 32, come in the wake of the exploitation of a critical vulnerability in HyperVM, a virtualization

https://www.theregister.co.uk/2009/06/09/lxlabs_funder_death/

VULNERABILITY -> HACK -> OUT OF BUSINESS -> DEATH

OTOH: hype is tempting. But not constructive.

Bloomberg

SUPERMICRO

■ October 4, 2018, 11:00 AM GMT+2

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.

https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

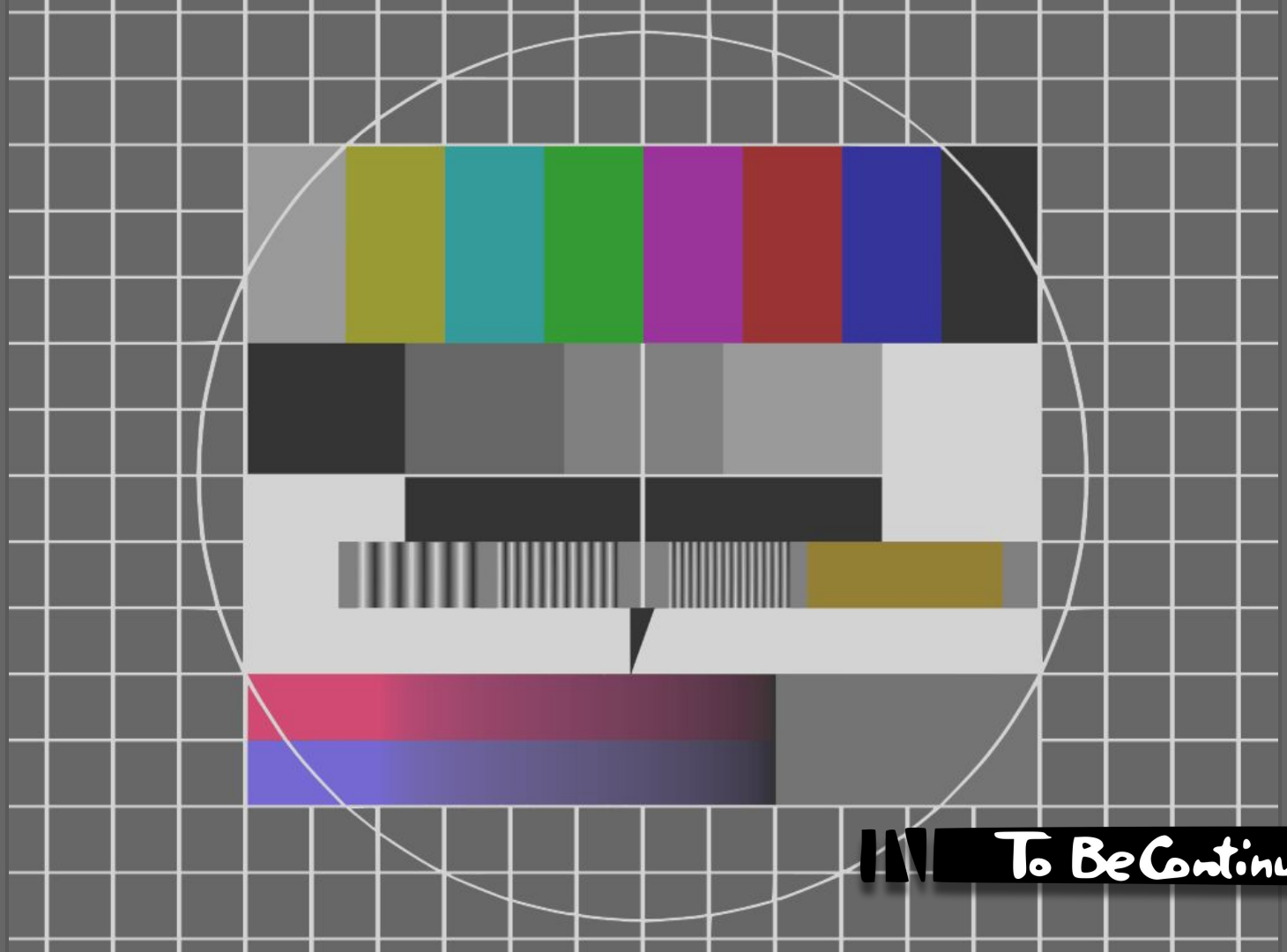
https://twitter.com/slekies/status/1052467737094746113

Unpopular opinion

InfoSec is in its early teens.

Still immature:
too much self-promotion, too much bugs fetichism,
still blaming others.

Story time


To Be Continued


YOUR MISSION:
EXPLAIN MELTDOWN TO YOUR ... GRANDPA / BOSS / KID.

Available online material are **very** limited.

To say the least :D

Hardly re-usable for experts :(

Hardly anything useful for teaching?

Too complex, too much Jargon.

Too much self-promotion. Buzzword and hype.

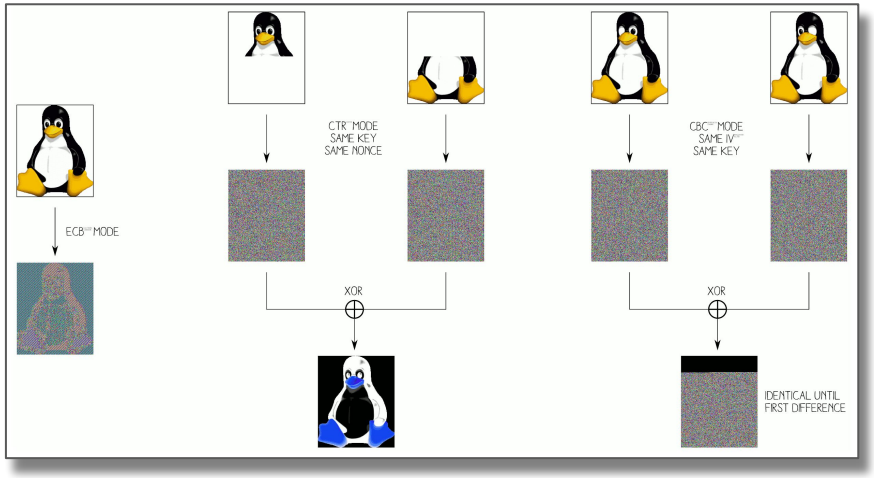
TMA-2KTO: Too Many Acronyms To Keep Track Of.

Story time

Documentations scales.

Not rewarded professionally.

No direct feedback, so it feels useless.



Writing accessible documentation helps everyone: it **scales**.

Stop the blame game

The tools for learning are abundant.
It's the desire to learn that's scarce.

- Naval Ravikant

More like: the docs/tools for learning already require expertise.
Hey, I wrote this. RTFM!
"I blame them for not reading everything I wrote".

Story time

Documentations doesn't raise stock price

Corporate environment favors measurable short-term goals:

-> Totally the opposite of documentation writing.

What's the "**COMPUTER SECURITY KIT**" for kids/users?

Any peg board game to teach kids basics?

Any 'dual raspi' distribution to learn security?

We need to demonstrate more.

Show how trivials things are.

It's the same old bugs all over again.

There's no wikipedia for infosec :(


F
To Be Continued

Another problem...

"Hey, I wrote about this topic already!"

"old is new again" doesn't mean it's bad.

Potential reasons:

Impostor syndrome?

We don't value our knowledge well enough ("not worth sharing".)

Immaturity?

Novelty addiction.

http://stuffman.tumblr.com/post/92082212353/people-have-written-a-lot-of-touchy-feely-pieces

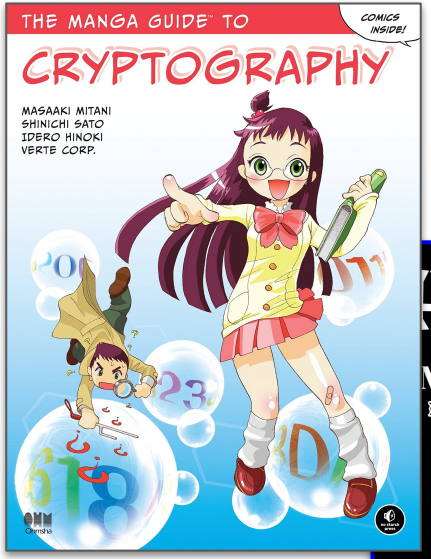
Story time

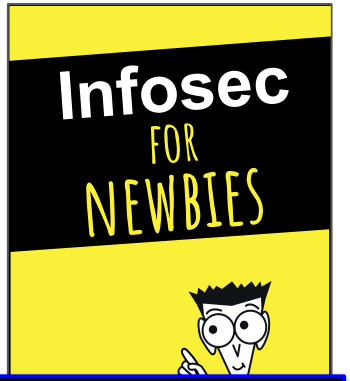
We often forget that...

Just a different style can make things click.

And a different style can reach different users!
We all had a bad teacher about something we love,
or a great teacher for a topic we usually hate.

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





https://www.getdigital.de/Hacken-Open-Air-Shirt.html?her=BB

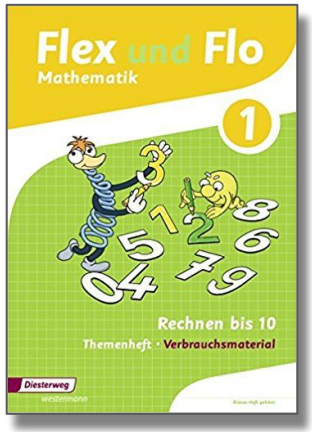
Story time

Unpopular opinion

It's OK to write about something that is already documented.

We still teach that 1+1=2. There are even **new** books for that.

Just don't claim it's new. It's not a shame.
InfoSec just needs to scale its knowledge.



The Internet is full of fake resources

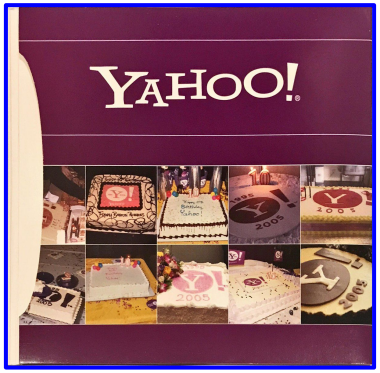
"Buy our stuff!"

- Snake oil
- Fear, Uncertainty and Doubt

http://cargocollective.com/samgray/Snake-Oil

"...nobody ever got fired for buying IBM equipment..."

Self-flattery

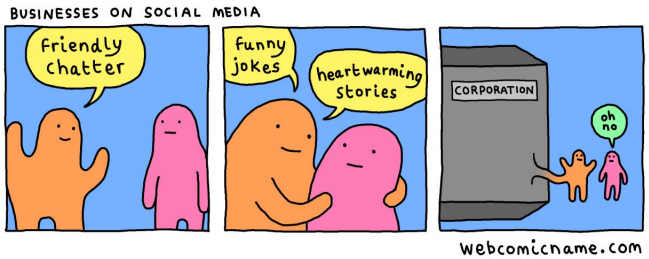


Yahoo 10 years

"We're so cool"

- Disguised marketing
- Digital sociology: observe, hype, don't take action.
- The show must **stop**.

They believe us now. We can evolve now.



http://webcomicname.com/post/154211839894

Common styles of "education"

- Belittle, blame, shame.
- Spam, bore.

And yet, shaming/scolding "works", but...

Fear or Trust?

Self-doubt -> loss of control -> authority.
Losing control of yourself seems to give faster results,
But it makes your audience stop listening.
They're just obeying and fearing.

"The best political weapon is the weapon of terror. Cruelty commands respect. Men may hate us. But, we don't ask for their love; only for their fear."
— Heinrich Himmler

Story time

We're in the same boat

- Show you care. Suggest > lecture > blame.
- Seize the opportunity: The brain is not always available.
- Guide and let find.
- Make receptive, then share experiences.

Yes. It takes time and effort. But it's rewarding.

Story time

Shotokan fellows

Education = make understand

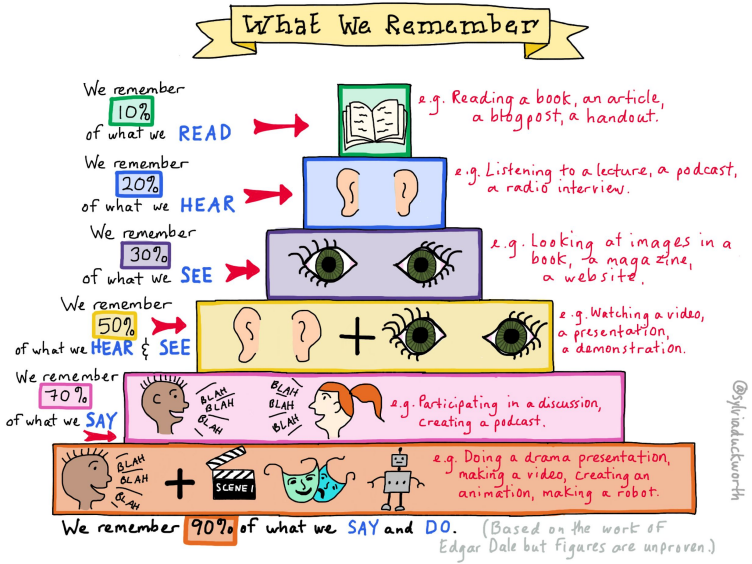
Make them fear the risk, not the teacher!

Connect. Simplify (but make clear it's simplified)

A Proof Of Concept is worth 100 words.

Give a sense of risk <-> security

"...you won't believe what happens next..."

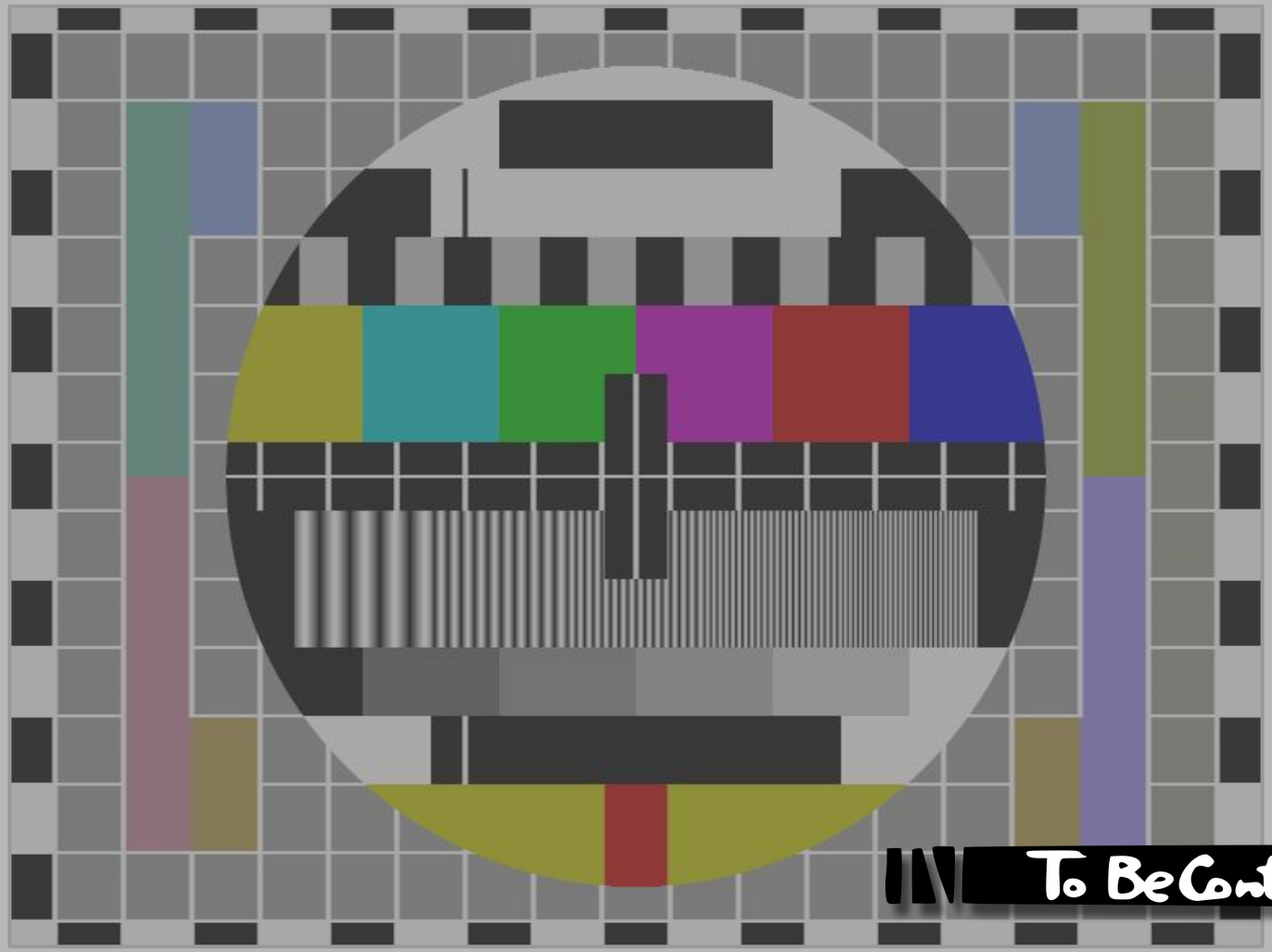


Story time

NEW SLIDE

In case you fail to keep control

To regain trust,
quickly provide a honest **post-mortem**
with sincere apologies to clearly explain what happened.


To Be Continued

One more thing...

Education is not limited to classes or training.
Every action is a vote:
favoring something puts weight into it.

We all have potential *followers*:
colleagues, peers, friends, family.
What you *do* inspires people, even unwillingly.

Actions outrank tweets

It's easy to be an actor and to pretend while on a stage.
It's much harder yet much more **powerful**
to change your local environment.

You don't need to be "important" or "famous" to educate people.

Changing *"only"* your surroundings
can have more impact than
reaching a wide audience at a major event
(that maybe listens but doesn't relate).

We know that things are broken.
We keep proving it. But to **ourselves**.

Talks/blog posts/magazines only reach our community.

We need documentations. Better kids book.
Simple website. Pedagogic examples.

Next evolution of InfoSec: resharing old stuff in better way.

Beyond CVSS score, what's the pedagogic impact of a vulnerability?

Story time

Conclusion

Leave your ivory tower.

You're not leet. They're not all idiots.

Better communication helps

To convince your management too - and defense is political!

Novelty shouldn't be the only focus.

Existing knowledge is overlooked..

Share known facts better.

Talks only reach our community.

Writing docs is ungrateful.

...until the next evolution!

Thanks!

Feedback?

Acknowledgements:
Thais, Phil, Gynvael, Mathieu, Axelle, Guénaëlle, Claus.

ANGE ALBERTINI
reverse engineering
VISUAL DOCUMENTATIONS
@angealbertini
ange@corkami.com
http://www.corkami.com