Hack In Paris

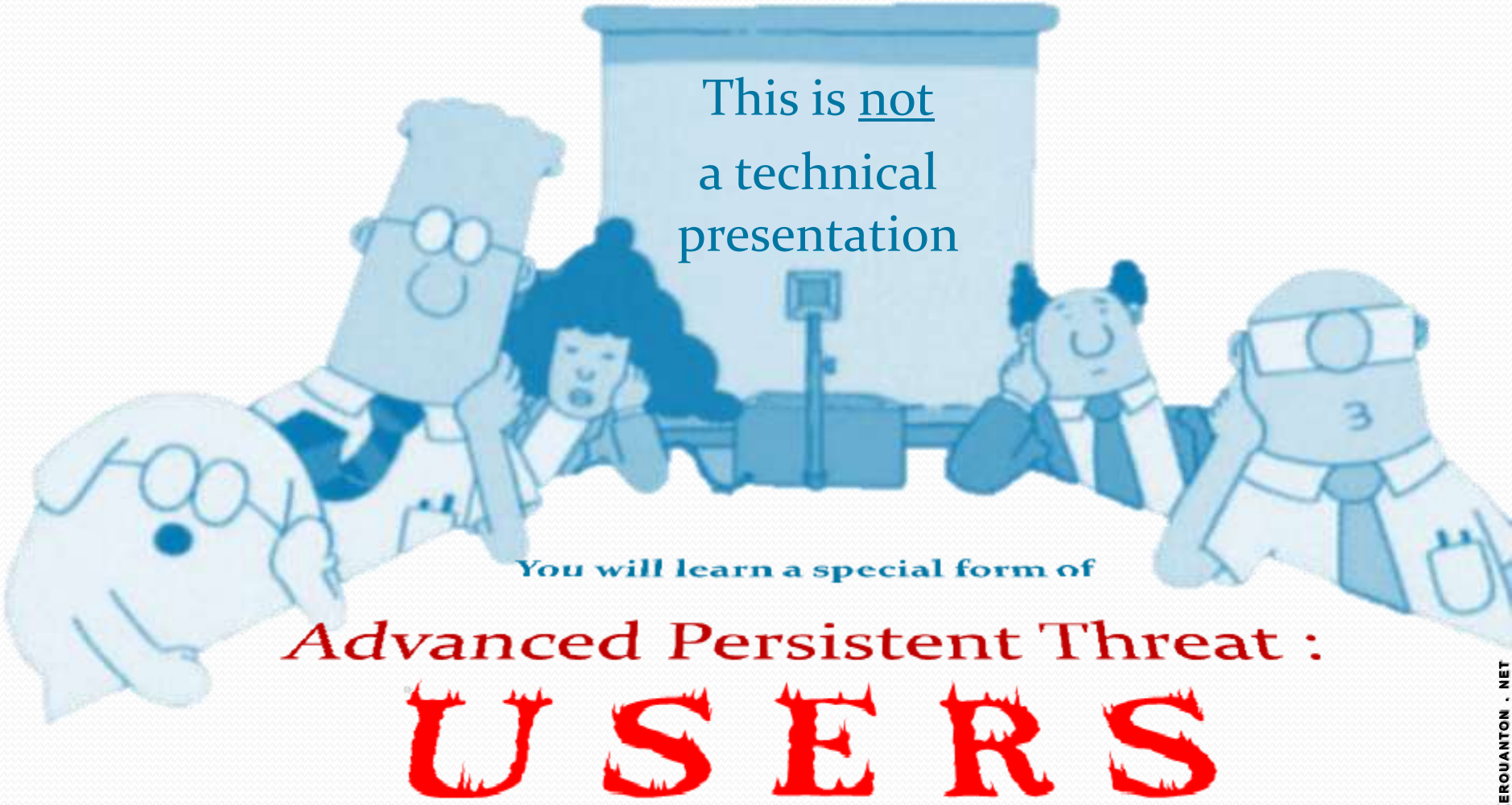
Be a smart CISO, learn about people

by Bruno Kerouanton

HACK IN PARIS

June 2011 - Disneyland Paris

Disclaimer


This is not
a technical
presentation
You will learn a special form of
Advanced Persistent Threat :
USERS
©2011 Bruno Kerouanton . net

I. How

Some facts about psychology

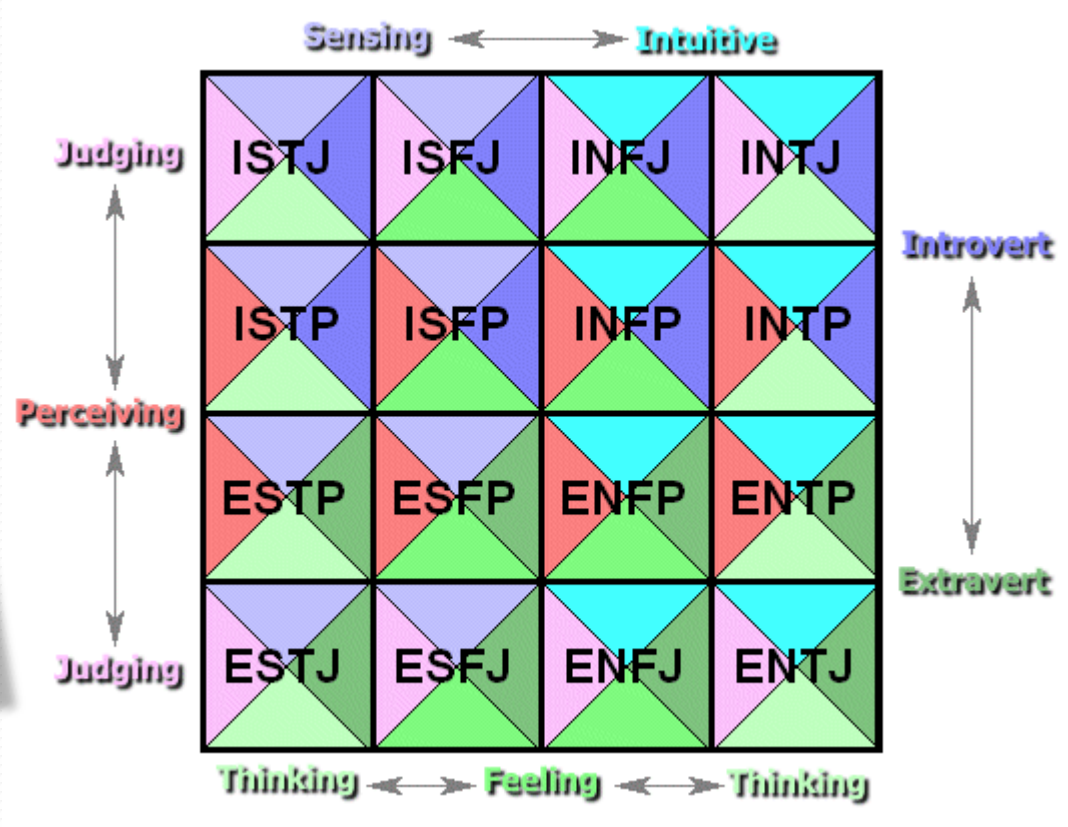
Explaining magic tricks

Magicians and mentalists mostly rely on human behavior predictability…

…as pentesters rely on TCP sequence predictability !

Classifying personality types

- Anyone seen this chart before ?



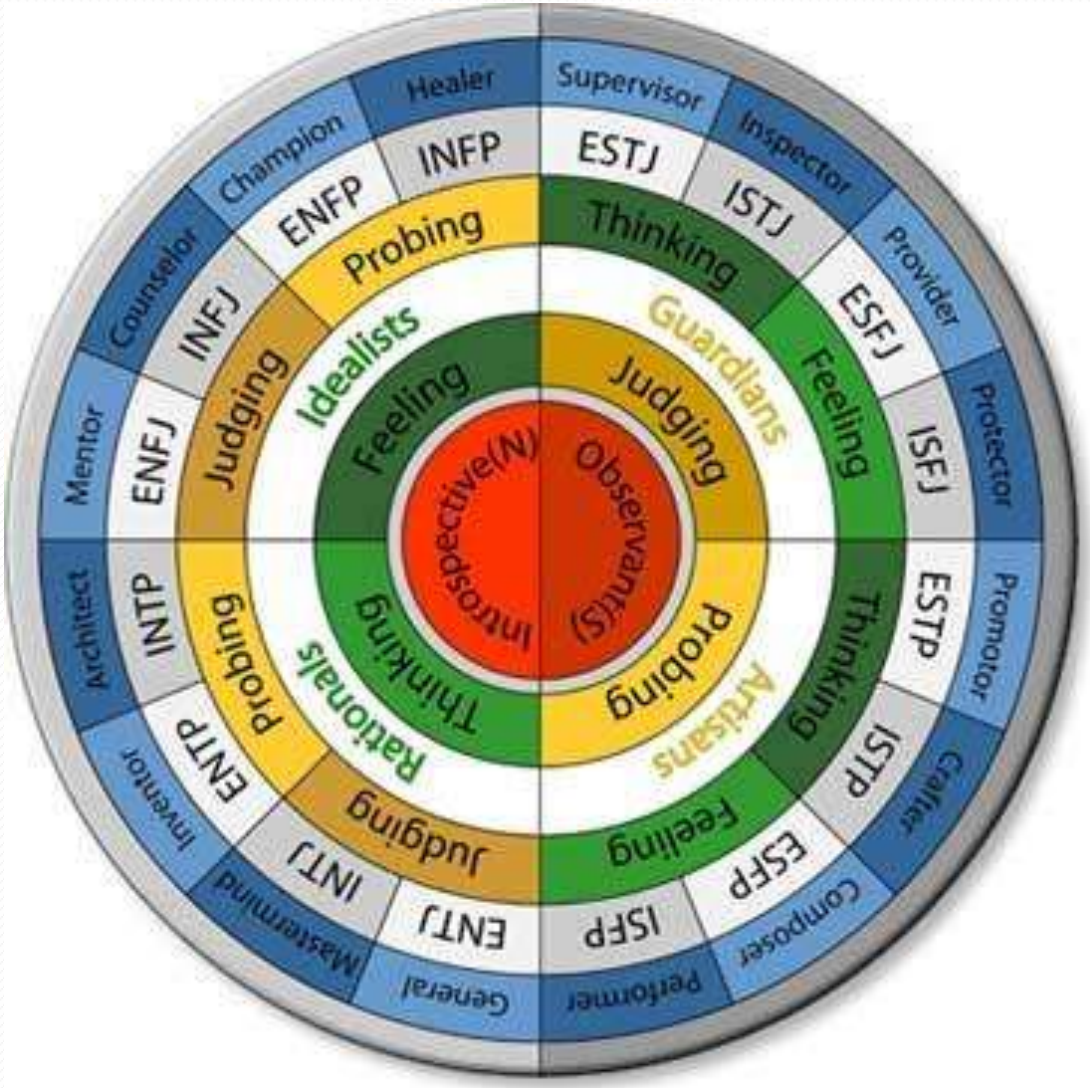
The Myers-Briggs typology (MBTI)

Initially defined by Carl Jung

16 types of personalities

A quick'n'dirty way to «put someone in a box»

Use it with caution : it's not an exact science !



Let me guess about you…

The Barnum effect

«Many people tend to believe any generalized description of themselves, given by an authoritative source.»

Very useful for magicians, circus, and horoscopes !

But also for you !

Let's summarize

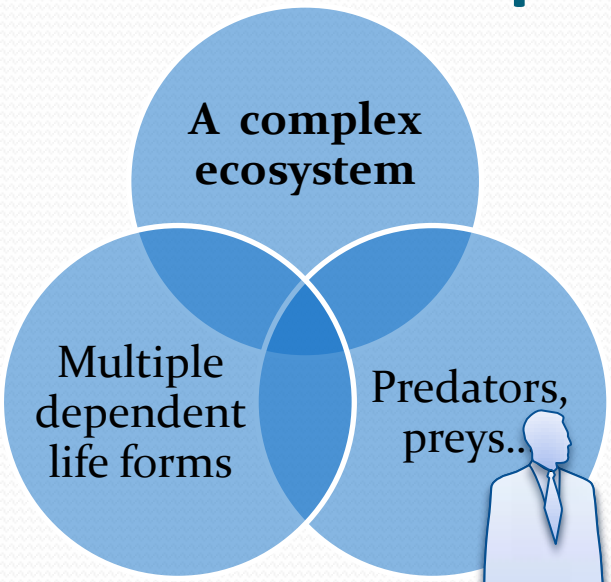
Fact one **Categorize**	• It's easy to categorize people. *(more or less)*
Fact two **Convince**	• It's easy to convince people that we know them, once categorized.
Fact three **Predict**	• It's easy to predict people's behavior.

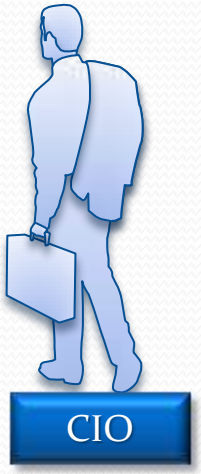
It's only about methods, not magic

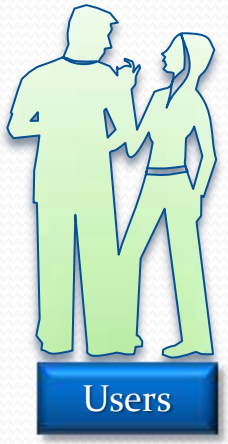
2. Who

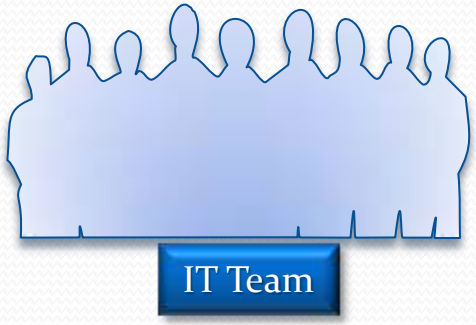
are you gonna deal with today ?

Your corporate environment









Chief Executive Officer

VIP End-user

Difficult to reach

Security is your problem

Has got the budget

Can support your plans

Need security

Treat any Executives as they deserve it : V.I.Ps – They feed you daily !

Be factual and smart when in touch : plan your “business case”

They need you, even if they don’t like to say it. Bring them what they want.

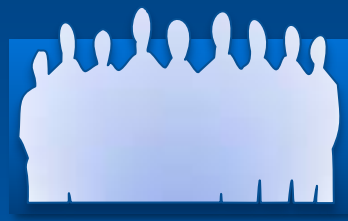
Chief Information Officer

Has his own goals	Can help a lot if partner
Can be against you	Understands IT
Won't always share budget	Need security

The CIO wants his IT to work, not to be slowed down by security.

You can delegate security to IT only if you help the CIO reach its objectives.

Don't do the work twice, and be careful not to be "eaten" by IT.



IT team

Does not always follow you	Can be motivated +trained
Wrong angle for security	Can help to do security
Have superadmin rights	Need security for systems

You have to establish good relations with IT teams. Meet them at coffee breaks.

Establish a direct link with them, for quick feedback… and delegation.

They have way too much rights. Focus on their workplaces and train them.

Often too busy for you

Have admin rights on users

Often outsourced/students

The best incidents source

The best contact with users

Need security to help them

Helpdesk is your main/best way to interact with users. Don't neglect it.

Train them if possible, and take care of them to let them feel accompagned.

The more they like you, the more security will be enforced at user lever.

Externals + Trainees

They are like Cancer !

They spread everywhere

Once they know they leave

Good incentive for you

Can bring new ideas

Keep you awake

Be strict about rules enforcement, setup a basic training with HR.

Look at their vision of security.

From time to time, hire trainees/students in your dept and discuss with them.

End Users

Reluctant to change

Underestimates security

Believes it's IT's problem

They have time for you

They can help you

Users have PCs at home

Build a positive image and a strong reputation (actions, trainings, press).

Rely on users, convince them to endorse the security with you.

Teach them about security at home, they'll apply it at work.

Let's summarize

Organize	• Organize your relations with people.
Convince	• Convince everybody, from the CEO to the users.
Lead	• Establish a strong image, be someone people can count on.

People will help you. Communicate !

A problem has been detected and Windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

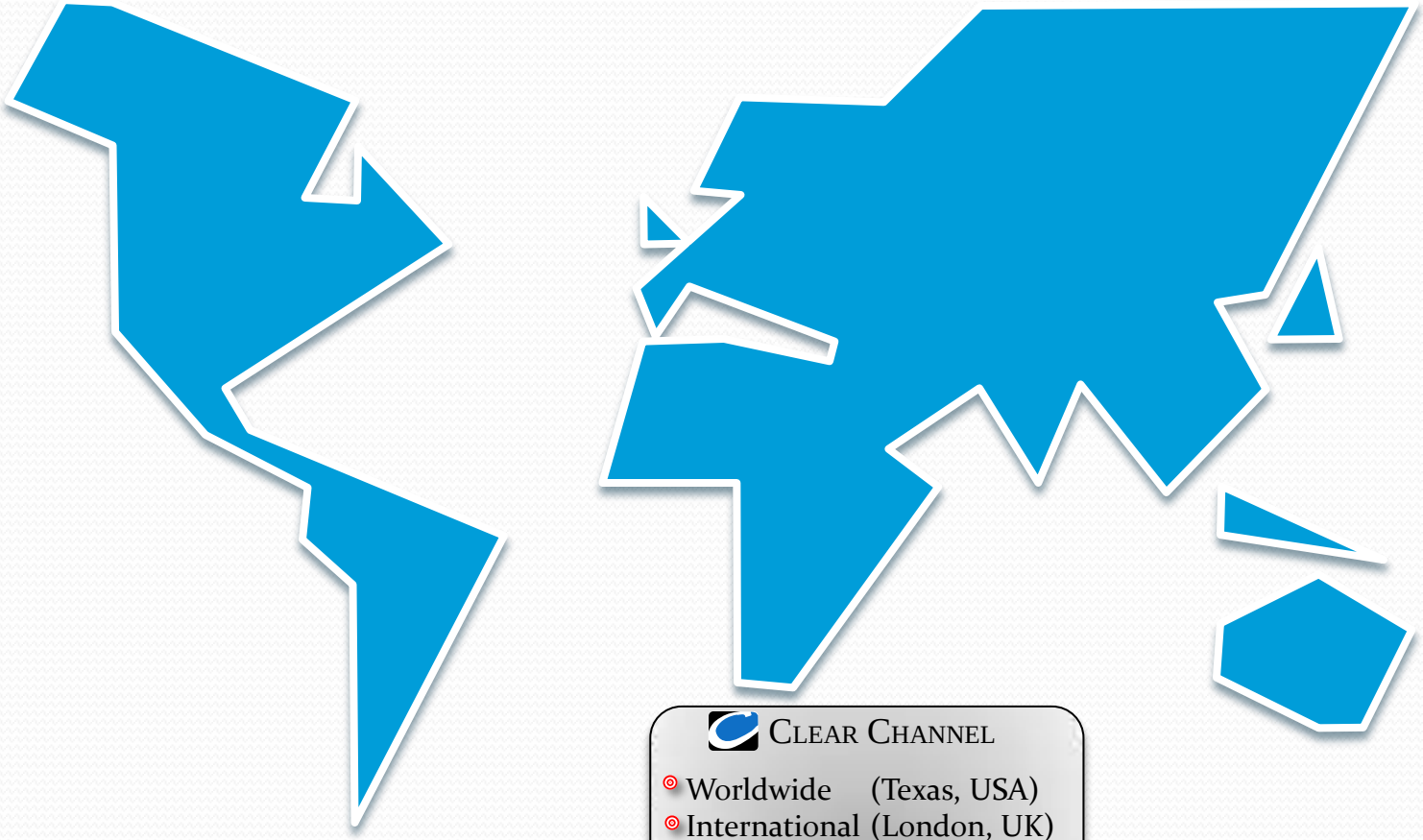
*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)

*** SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c

3. Facts

my experience from around the world

Small CISO, big company…



Being a CISO in an globalized company

- I was officially attached to the local French CIO

but

- Strong commitment with the French executives (CEO, CFO…)
- And receiving orders from Texas, *via* London

This was my 1st lesson about *Power* and *Ties* between people

What did I learn

French CIO
French Executives
London

Fr. Executives
London
Texas

French,
Englishmen
and Americans

have different

languages,
cultures
and vision.

So I leveraged those behaviours

Republic and Canton of Jura

A sovereign republic created in 1979

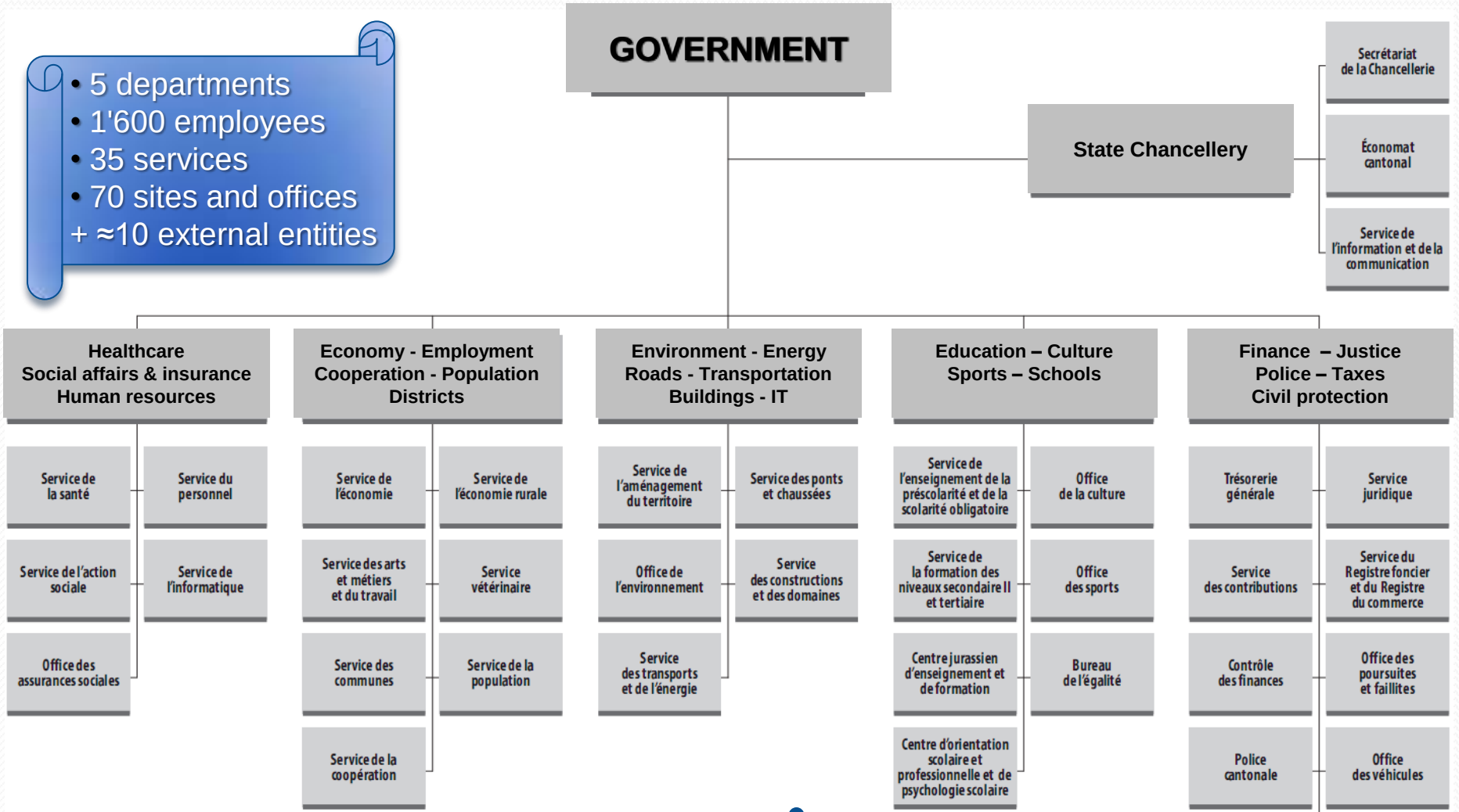
- Area : 838 km²
- Population ≈ 70'000 citizens
- Density : 83 / km²
  (1 football field per citizen)
- Language : French
- Capital : Delémont

- Government : 1 president,
  5 ministers,
  1 chancellor.
- Parliament : 60 deputies.

A complex and political environment

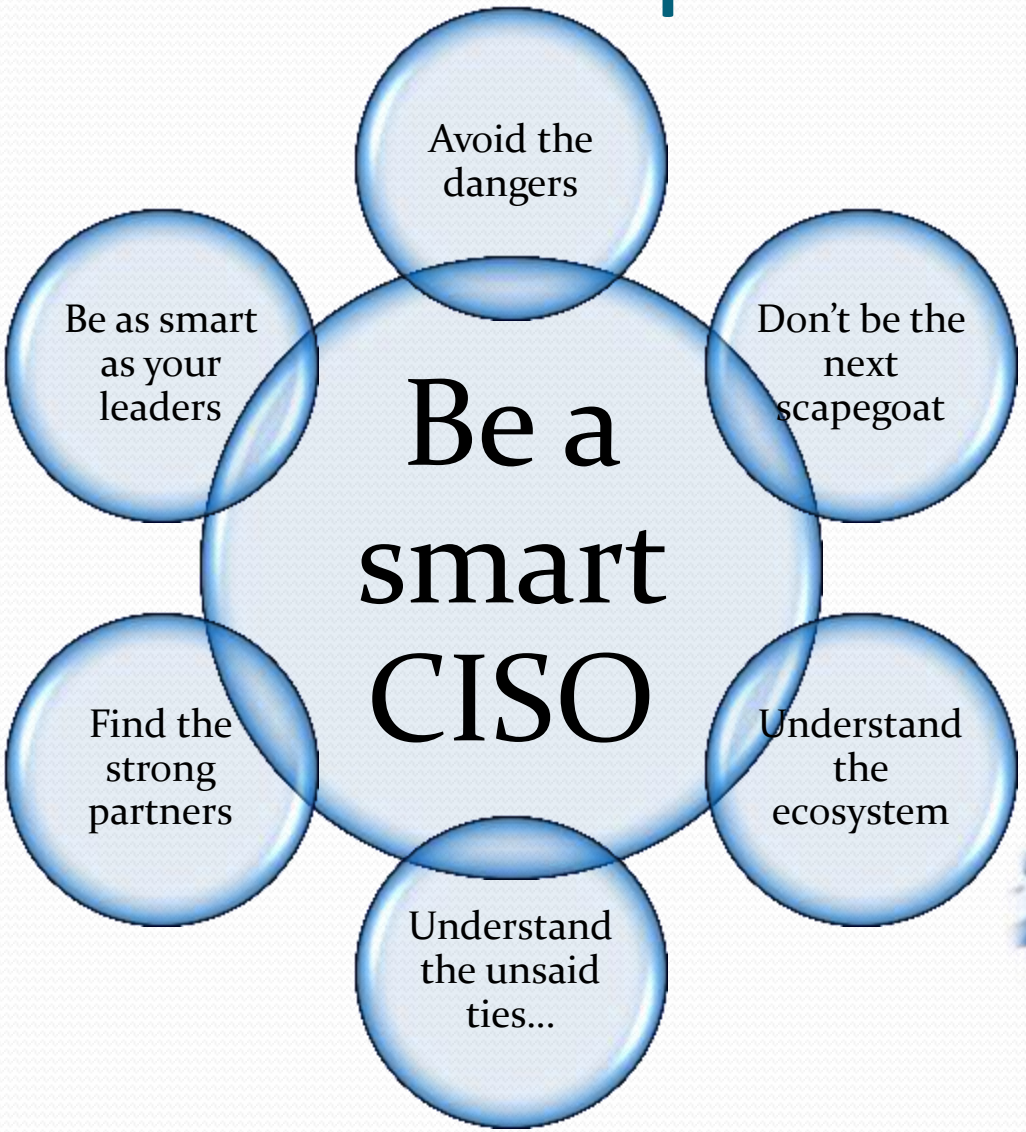
- 5 departments
- 1'600 employees
- 35 services
- 70 sites and offices

+ ≈10 external entities



A **huge** challenge for IT security !

Threats and politics



Let's summarize

Fact one
Understand

- Understand the inner workings of your organization, and all the invisible ties.

Fact two
Associate

- Partner with people other than IT and your boss, establish your own ties.

Fact three
Empower

- Make those persons help you and act together to enforce security.

There is no thing such as relations

Your company is a lab !

So let's apply what we've learned here !

Your given objectives

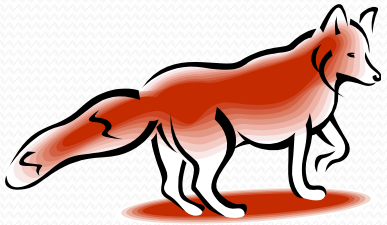
Ensure corporate security and repel villains.

Spend as little money and resources as possible.

Work very hard to handle everything at once.

Follow the orders, don't bother the CEO nor the CIO.

Your (real) objectives



Power

tay … he
comp … y
s lo… … s
you … .

Get all the budget and resources yo… need

… egate as much work as you can.

respected and listened.

Simple and pragmatic : it's all about …

It’s all about politics… too

A company is a political arena

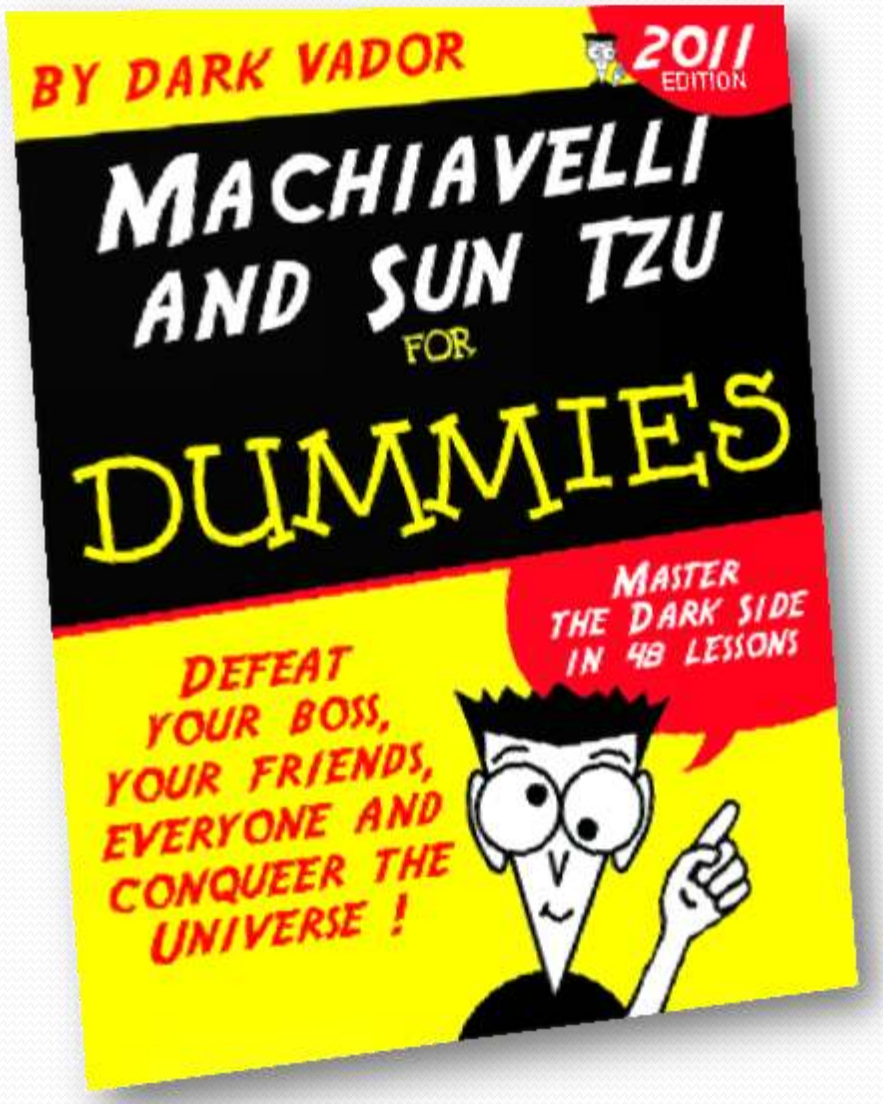
The more you have responsabilities (CISO, CSO),
The more you walk on eggs…

Being a CSO requires political skills :

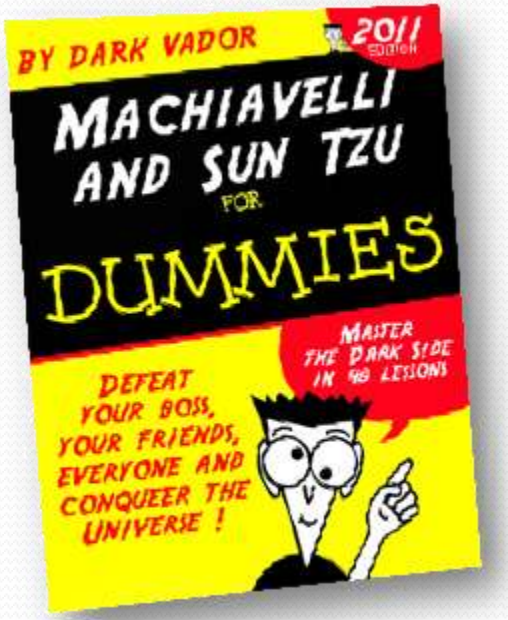
Communicate – Be a leader – Have a vision

BE THE FOX AND AVOID THE WOLVES : BE SMART

Would you like to get this book ?



The 48 laws of Power, by Robert Greene



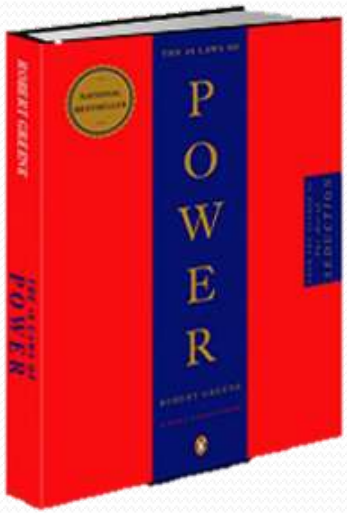
I. Never outshine the Master
II. Learn how to use enemies
III. Conceal your intentions
IV. Always say less than necessary
V. Your reputation is gold

VI. Court attention at all costs
VII. Get others to do the work
VIII. Make people come to you
IX. Use action, not arguments
X. Avoid unlucky people

Et cætera…

The 48 laws of Power, by Robert Greene

Well, this book is a must-read.



But, please…

stay on the **good** side of the Force

And finally, be charismatic !

- Build a strong image of you
- Give actions, not talks
- Never outshine the Master
- When lost, re-read the 48 laws of Power

And each morning you'll be *happy* to get to work

I hope to see you soon in Jurackerfest.ch !

The Swiss Jura Hackerspace Festival

26 and 27 august 2011