TLP : CLEAR

Cybersecurity: bluster industrialists and craftsmen of the unexpected

Inti Rossenbach

2 October 2025 – CERT-EU Annual Conference 2025

01

Amoral uncertainty of risks

02

Poison of bureaucracy

03

Fantasy of industrialisation

TLP : CLEAR
(original TLP was AMBER: some sections are redacted – in black, interesting oral comments)

whoami

Group CISO – Insurance brokerage, 7000+

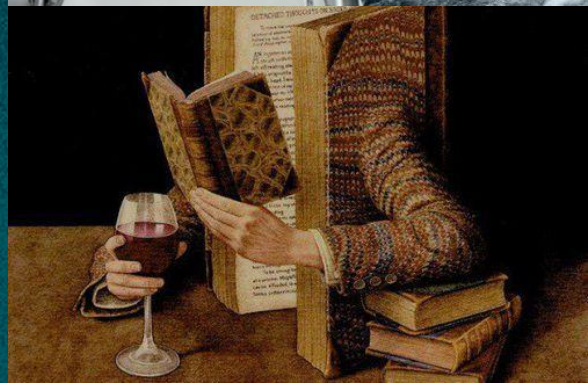
Infosec practitioner since the last century

Lecturer at university

https://www.cryptosec.org
– my good old website, handmade, up since year 2000

iro@cryptosec.org
https://infosec.exchange/@cryptosec

my own views –



TLP : CLEAR

01 Amoral uncertainty of risks

TLP : CLEAR

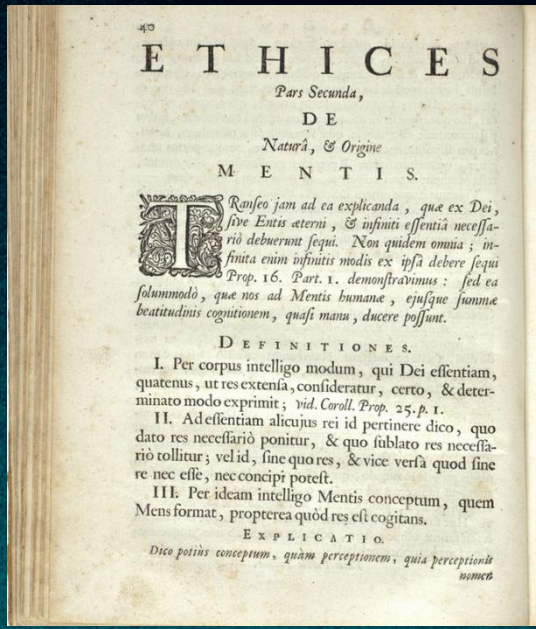
Amoral uncertainty of risks

Risks are very often considered from an implicit **moral** standpoint: they are bad, **security is good**

It is reassuring, but it is false: there is no life without risks – **risks are the counterpart to life**

Reducing risks is often perceived as an easy antidote to one of Spinoza's sad passions, **fear**

Security is costly – money, energy, time, usages and freedom



40

ETHICES

Pars Secunda,

DE

Naturâ, & Origine

MENTIS.

Transeo jam ad ea explicanda, quæ ex Dei, sive Entis æterni, & infiniti essentiâ necessariò debuerunt sequi. Non quidem omnia; infinita enim infinitis modis ex ipsâ debere sequi Prop. 16. Part. 1. demonstravimus: sed ea solummodò, quæ nos ad Mentis humanæ, ejusque summæ beatitudinis cognitionem, quasi manu, ducere possunt.

DEFINITIONES.

I. Per corpus intelligo modum, qui Dei essentiam, quatenus, ut res extensa, consideratur, certo, & determinato modo exprimit; *vid. Coroll. Prop. 25. p. 1.*

II. Ad essentiam alicujus rei id pertinere dico, quo dato res necessariò ponitur, & quo sublato res necessariò tollitur; vel id, sine quo res, & vice versâ quod sine re nec esse, nec concipi potest.

III. Per ideam intelligo Mentis conceptum, quem Mens format, propterea quòd res est cogitans.

EXPLICATIO.

Dico potiùs conceptum, quàm perceptionem, quia perceptionis nomen

How to assess risks ?

People are usually much more convinced by numbers than by words: numbers seem more “real”, they smell science

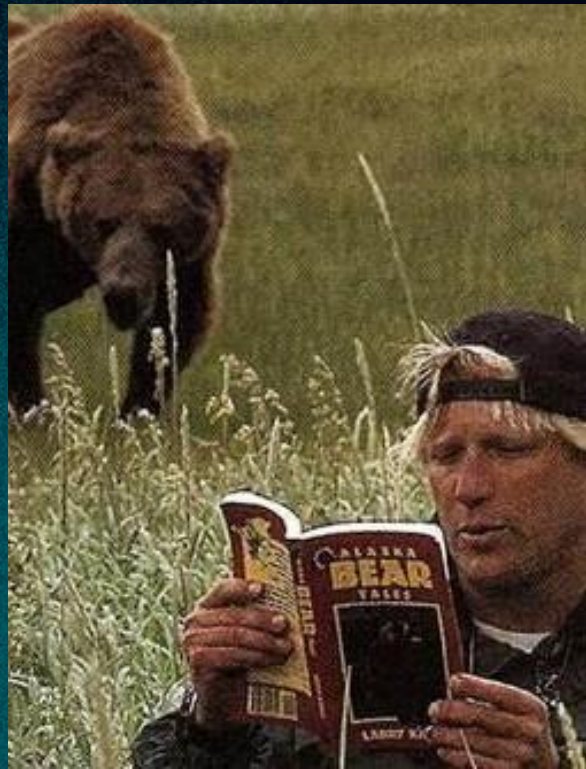
But each time you see something like “70% of intrusions occur from within the organization”… you should say: probably fake

How can we make **rational decisions** when we have little or **no statistics** ?

We must rely on **qualitative statements**, experience, expertise, approximations, and orders of magnitude

And that's not a bad thing. That's where honesty and our freedom of action and decision-making lie

Rather than KPIs, KRIs… PowerPoints, we have to rely on **reasoning and sentences**



TLP : CLEAR

Conservation of risks

Reducing a risk does not eliminate it, in general

Often, **reducing** a risk **creates other risks**

We do not have sufficient budget !

Despite our ego, we always have to remember that we are a **support function**

If you don't have enough resources, it may simply be that your organisation is **ready** to **take higher risks than you imagine**

Just say so. It is neither good nor bad in itself

```
Action Required: Data Breach Notification

Your Data Is Now Beyond Your Control

We have taken control of your systems, encrypted your
critical files, and extracted sensitive data. This is a
pivotal moment for your organization—your actions now
will determine the outcome.

---

What You Need to Understand
Your data security was compromised because of
insufficient protection. As a result:
1. All access to important files has been restricted
through encryption.
2. We possess confidential business records, personal
data, and other critical information.
3. If you do not respond within 72 hours, we will
initiate the public release of your data, creating
irreversible damage.

---

The Risks You Face:
Failure to act swiftly puts your organization at risk of:
- Legal violations under GDPR, GLBA, CCPA, HIPAA, NYDFS
Cybersecurity Regulation, and DPA 2018.
- Financial penalties for failing to protect Non-Public
Information (NPI).
- Reputational harm as clients, partners, and the public
lose trust in your ability to safeguard their data.
```

31 January 2024

Massive data theft from 2 leading provider of third-party payment and direct healthcare payment *(Tiers Payant)*

Attack began on January 22

We are the client. They process our data…

[REDACTED]

TLP : CLEAR

Doubts on the modus operandi –

A massive data extraction ? How ?

An intrusion ?

But again, we have this…

[REDACTED]

TLP : CLEAR

2 February – Internal statement – *CISO to EXCO*

« ... these informations do not allow to exclude an intrusion. However, it's very unlikely. »

2 February – Our public com'

« Consequently, we considered that there was no justification for cutting the links with our third-party payment operators and that such an overreaction could, on the contrary, cause unnecessary inconvenience for our customers, beneficiaries, and partners. »

Reducing risks by cutting the link was not the *good* option

It would have created another risk (for clients): unavailability

Our risk assessment was not quantitative

The company was OK with our risk-posture proposal

02

Poison of bureaucracy

Organisations generate bureaucracy

While we are familiar with alert fatigue… let's talk about *bureaucracy fatigue*

TLP : CLEAR

What is bureaucracy the name of ?

Heaviness and rigidity... it’s a form of work organization

- A desperate attempt to bring certainty in a landscape of uncertainty
- Monopolisation of power
- Other's processes
- Another name for... lack of trust

Formal and informal bureaucracy

Formal : complex policies & processes, validations, hierarchy, controls, reporting, certifications, compliance, regulation, etc.

Informal :
- Fear of taking responsibility
- Lack of trust
- Parkinson's law of triviality: organisations commonly give disproportionate weight to trivial issues

To each his own bureaucracy

- Massive organisation
- Useless jobs
- Change & incident tickets
- Requests to suppliers/support
- Pointless meetings / Flood of emails
- RACI matrix
- Budget “engineering” & approval
- Use of slides – when appearance matters more than substance
- Control (*a priori* rather than a posteriori)
- Decision making
- Security reporting
- Management: timesheets, annual reviews, performance reviews, recruitment...

Some slides ago I mentioned « Regulation » as a sample of « formal » bureaucracy.
It is indeed a source of bureaucracy.
But we also really need regulation: without regulation, the « free market » leads to concentration, abuse of dominant position, waste, failure to respect privacy

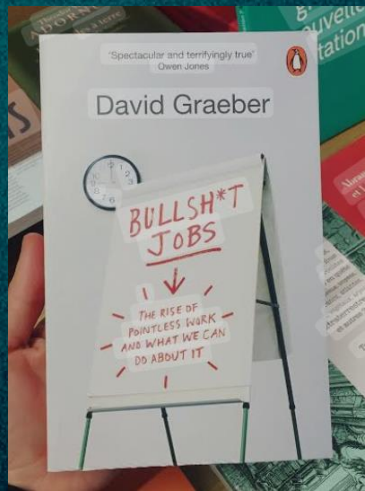
Public sector vs. Private sector

Private companies are just as bureaucratic than public entities, sometimes / often more

Other names: management, policies, process, reporting, control, quality, audit...

Hypotheses (Graeber):

- Profit: sanctions, fines to those who do not respect the “rules”
- Justification for the existence of... bureaucrats
- Lack of trust



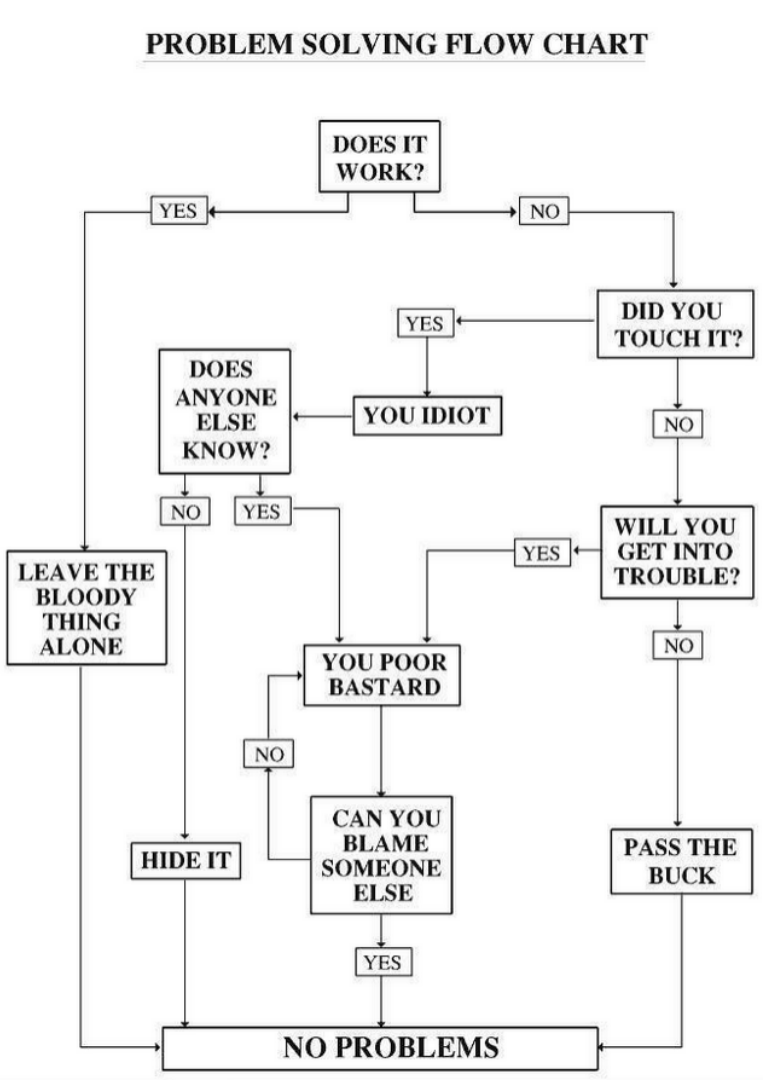
Focus on policies & processes

They are necessary

The problem is that often:

- Belief that a task is done/managed when the process is written down

- They can turn the organisation too rigid and unable to transform quickly when needed, for example in the event of a crisis



6 consequences of bureaucracy

- Costs and delays
- Dehumanisation
- Demotivation
- Distortion of risk perception
- Unnecessary risk-taking (e.g. shadow IT)
- Rigidity – difficulty in dealing with the unexpected

BTW, what is the etymology of this word ?

Bureau _ Office

-cracy [ancient Greek]
rule (in the sense of governing)

From *bureaucratie*:

it's a French word \o/

03 Fantasy of industrialisation

Industry ?

“IT industrialization is the standardization of IT services through predesigned and preconfigured solutions that are highly automated, repeatable, scalable and reliable, and that meet the needs of many organisations”

Gartner

In this definition from the Gartner, something is missing.

Costs.

The main objective of industrialisation is cost reduction.

While bureaucracy has a bad connotation, industrialisation almost always seems virtuous

What does the industry produce : standardised products, whose manufacturing processes are driven by cost reduction (taylorism, fordism, offshoring, lean management, etc.)

Industry ?… like…

Cars you cannot fix – have you ever tried?
Awful clothes, made by exploiting people and destroying the environment
Do you really beleive the Billy bookshelf is a good product?
Do you really beleive mass production is something good to us… and our children…

TLP : CLEAR

Industry or craftsmanship ?

Automation is essential, at the heart of all IT activity

The benefits of industrialisation are almost always those of the supplier or service provider, not those of the user, customer or citizen (e.g. cloud)

If you want a complex product or service **that meets your needs**, it is probably better to opt for handmade. Which can use industrial components

It may be more expensive. Or not. But it is more durable, can be of better quality… and can meet your needs, address your specific risks

This applies to food, clothes, handbags, bookcases... or infosec / cybersecurity

Complex objects, of high quality, which fit your needs are not mass-produced or standardized.
You may say… and iPhones?
The magic here is that industry often manage to convince us that we need their production
Industry creates our needs

TLP : CLEAR

Operational security

Good prevention, detection, investigation and response processes are essentially artisanal, handmade
Because they deal with the **unexpected**

We know this

But we must learn to accept it: we are craftspeople, artisans. Good services are expensive and require skilled people, not industrial assembly lines

Cybersecurity is not an industry

TLP : CLEAR

[REDACTED]

TLP : CLEAR

Incident context

[REDACTED]

TLP : CLEAR

Incident timeline

[REDACTED]

TLP : CLEAR

TLP : CLEAR

But how did that begin?
A chaotic series of fixes...

Signs of major design weaknesses… what are Perl and Python interpreter doing on this kind of appliance, for instance?
And I know that there are people in this room who had access to the core of these appliances, among others, and… c'est pas joli joli.

10 January
CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) | Mitigation but not a remediation

10 January
Volexity: Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN

15 January
Volexity: Ivanti Connect Secure VPN Exploitation Goes Global | Integrity Check Tool | 1,700 devices compromised

18 January
Volexity: "Ivanti Connect Secure VPN Exploitation: New Observations" | non-public exploits | 2100 devices infected by a webshell

22 January
CVE-2024-21888 Privilege Escalation for Ivanti Connect Secure and Ivanti Policy Secure | new vulnerabilities

31 January
CVE-2024-21893 and new patch

1st February
a new cumulative patch

I am sure that a VPN gateway maintained "artisanally" by experts, handmade in the better sense of the word, would not have suffered such weaknesses.

This IS NOT a device manufactured by an industry

This IS a device manufactured by an industry

Our overall incident response was really handmade – in the best sense of the word

Handmade is everywhere, but hidden

Suppliers develop their products and services in a much more crafty way than they claim
Massive use of open source components developed and maintained very manually

- November 2021, Log4Shell
- March 2024, xz backdoor
- July 2024, CrowdStrike Falcon Sensor outage
- XXe century, Crypto AG - *“The intelligence coup of the century”*

Conclusion – 3 takeways

Security is not good in itself, risks are not necessarily bad, and most of the time we cannot quantify them

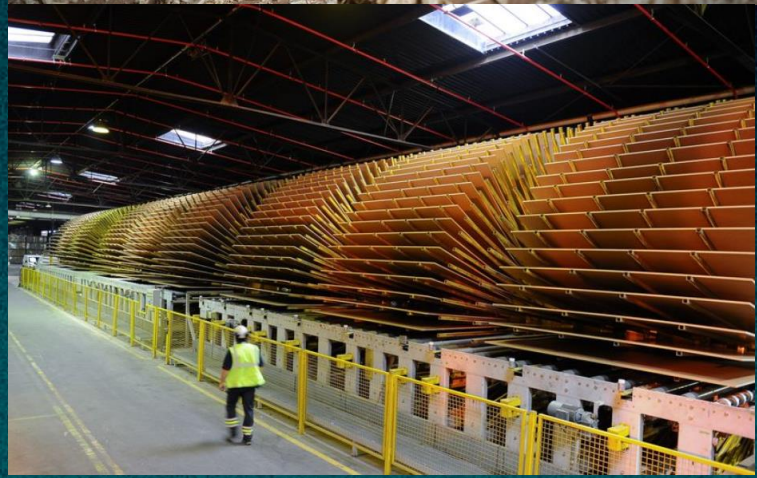
Bureaucracy is a sign of lack of trust – and that’s where the remedy lies

Conclusion – 3 takeways

Security is not good in itself, risks are not necessarily bad, and most of the time we cannot quantify them

Bureaucracy is a sign of lack of trust – and that's where the remedy lies

Infosec, cybersecurity is not an industry – we should embrace craftsmanship



Thank you for your attention

www.cryptosec.org
iro@cryptosec.org
https://infosec.exchange/@cryptosec

TLP : CLEAR