WEBINAR RECORDED

PECB

Closing the Decision Gap: How Risk-Informed Decisions Build Digital Trust

MAY 28 | 03:00 PM CEST

Christophe Mazzola

Founder / Trainer | Cyber Academy

#GlobalLeadingVoices

Agenda

1. The Decision Gap
2. Anatomy of Blockage
3. The Standards' Blind Spot
4. The Intervention Manual
5. From Auditor to Closer

PECB

PART ONE

The Decision Gap

A bit of cyberpsychology

WALLONIA · 2022-2023

An audit. One hundred administrations. One reply.

100	21	€1M	1,300
administrations	*auditors*	*budget*	*pages*

1 minister. 1 reply: “thank you.”

The report wasn’t wrong. The report was right. Three years later, most of those administrations still haven’t moved.

PECB

THE FRAME

Digital trust isn’t built when an audit signs off.

Digital trust is built when the decisions an audit triggers actually get made.

When they don’t, digital trust erodes. Silently. Cumulatively. Until reality cashes the check.

WHAT WE’LL DO TOGETHER

- A diagnostic grid: five blocking patterns, each grounded in a named cognitive bias.
- The structural blind spot in the standards we all certify against.
- An intervention manual: five protocols to close the gap.

PECB

FOURTH AND CLOSING EPISODE

Three symptoms. One disease.

IISF DUBLIN

Green dashboards

that lie

ISACA BELGIUM

Cyber governance

that fails

ESBG BERLIN

Algorithmic gaps

in banks

Today we name the disease, and we give you the protocol.

PECB

PART TWO

Anatomy of Blockage

Five patterns where recommendations die.

Real cases · NIS2 · ISO 27001 · ISO 31000

Nordelec, 2019. A 47-page ISO 31000 register.

Diffusion of Responsibility · Darley & Latané, 1968

“Pierre, you’ll look into options?”

“Yes, of course.”

Seven executives in the room. Each one assumed someone else owned the next step.

No deadline. No resources. No arbitration.

PATTERN 02 · ACCEPTANCE BY DEFAULT

A NIS2 gap assessment. Six months. Untouched.

Omission Bias (Ritov & Baron, 1990) + Status Quo Bias (Samuelson & Zeckhauser, 1988)

Same room. Same report on the table.

Untouched.

Nobody rejected the recommendations. Nobody accepted them. The silence was the decision.

The most dangerous decision is the one nobody made.

PECB

PATTERN 03 · POLITICAL COST

CPAS Charleroi. Public-sector NIS2-style audit.

Loss Aversion (Kahneman & Tversky, 1979) + Self-Image Protection (Steele, 1988)

The report wasn't wrong.

It was uncomfortable to sign.

End of August. Ransomware. The director went on national news: "We don't understand."

The comfort of inaction beats the discomfort of transformation. Every time.

PECB

ANTS · FRANCE · APRIL 2026

The same mechanism. At national scale.

11.7M

records exfiltrated

OWASP IDOR.

Documented since 2007.

0 action.

The debt wasn't technical. The decision-maker willing to attach their name to the fix never showed up.

Same cognitive math as CPAS. Across nineteen years and four governments.

PECB

Two faces. Same result.

Inattentional Blindness (Simons & Chabris, 1999) + Automation Bias (Mosier & Skitka, 1996)

RED WASH

47 pages.

23 risks. All "high."

Nothing extracted.

Nothing escalated.

Inattentional blindness.

GREEN WASH

1.48%

phishing failure rate · 12 months

Changed the simulator: 12%.

Automation bias.

Never triggered a decision.

PATTERN 04 · DROWNED IN THE FLOW

The CISO Dashboard Trap

What looks green and what it hides.

LOOKS GOOD ON THE DASHBOARD	WHAT IT MAY ACTUALLY HIDE
Fast MTTD	Long attacker dwell time before the first alert
Low MTTR	Delayed containment or partial remediation
High alert volume	Analyst overload and poor signal quality
Strong compliance score	Weak readiness against live attacks
Many tools in place	Fragmented workflows and slow investigations
Resolved incidents	Residual exposure or repeat activity

PATTERN 05 · UNTRANSLATED

The board doesn’t read 5x5 matrices.

Curse of Knowledge (Camerer et al., 1989) + Psychic Numbing (Slovic, 2007)

It reads scenarios.

Until the risk lives in the decision-maker’s language, it isn’t their risk. It’s yours.

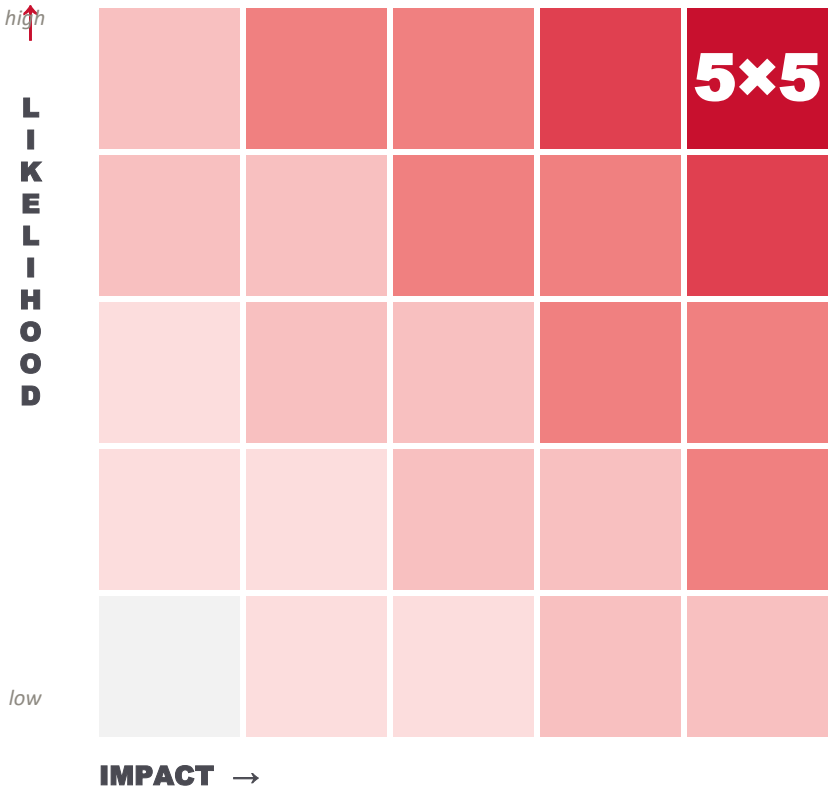
A matrix gets filed. A scenario gets decided.

PECB

PATTERN 05 · UNTRANSLATED

The board doesn’t read 5x5 matrices.

Lessons from Buenos Aires



Cybersecurity risk in 2024:

5 × 5

Cybersecurity risk today:

Still 5 × 5.

PECB

COGNITIVE SYNTHESIS

Five patterns. Five cognitive biases. One mechanic.

	PATTERN	COGNITIVE BIAS
01	Risk without an owner	*Diffusion of responsibility*
02	Acceptance by default	*Omission + Status quo bias*
03	Political cost	*Loss aversion + Self-image protection*
04	Drowned in the flow	*Inattentional blindness + Automation bias*
05	Untranslated	*Curse of knowledge + Psychic numbing*

Each blocked decision is a drop of digital trust silently leaving the building.

PECB

PART THREE

Why the Standards Won’t Help You Here.

The blind spot is structural.

Standards describe what. Not how to extract the decision.

ISO 27005 §8.6

"The risk treatment plan should be approved by risk owners."

How to obtain the approval against loss aversion and status quo bias? Silent.

ISO 27001 §6.1.3

Four treatment options. Modify, retain, avoid, share.

How to get someone to actually choose under cognitive pressure? Silent.

NIS2 Art. 20-21

Management bodies "approve" and bear ultimate responsibility.

What's the extraction mechanism when they avoid the meeting? Silent.

DORA Art. 5. ISO 31000 §6.5. Same gymnastics. Same structural gap.

THE CONCEPTUAL MOVE

Technical debt vs governance debt.

TECHNICAL DEBT

What code and infrastructure accumulate when shortcuts compound.

Solvable.

Time. Tools. Money.

GOVERNANCE DEBT

What an organization accumulates when decisions don't get produced.

Harder.

Changes how decisions are made.

ANTS in April 2026 wasn't technical debt. It was governance debt at national scale.

PECB

PART FOUR

The Intervention Manual

Five protocols to close the gap.

INTERVENTION 01 · DECIDE / SIGNS / OWNS

Three questions on every treated risk.

Counters: Bystander Effect / Diffusion of Responsibility

Who

DECIDES

the criteria, the threshold, the trade-off?

Who

SIGNS

the deployment of the mitigation?

Who

OWNS

the outcome when the mitigation fails?

If any column is empty, you don’t have a risk owner. You have an artefact.

PECB

INTERVENTION 02 · MAKE THE SILENCE SIGN

Inaction is a decision. Make the silence sign.

Counters: Omission bias + Status quo bias

THE OPT-OUT FORM

I am the named risk owner.

I acknowledge this risk at [level].

I choose not to treat it at this time.

I accept the residual exposure of [scenario / impact].

I will revisit on [date].

Signed. Dated. Named. Archived.

Most consultants don't produce this form for fear of refusal. The refusal IS the diagnostic.

The most powerful governance artefact in your toolkit is the signed acceptance of a risk.

INTERVENTION 03 · THREE SCENARIOS, NEVER ONE

Convert the binary trust vote into an executive judgment.

Counters: Loss aversion + Self-image protection

01

MINIMUM VITAL

Regulatory floor + existential risks.
Documented residual exposure.

02

RECOMMENDED

Your reference trajectory.
What you'd do in their shoes.

03

AMBITIOUS

Competitive edge.
Future-proofing. Posture.

Never embed a single recommendation. Three columns or none. The board's job is to choose.

PECB

INTERVENTION 04 · PRESSURE-TEST THE GREEN

4 questions. 60 seconds. Any green metric.

Counters: Inattentional blindness + Automation bias

Q1 **Who chose this metric?**

If the tool chose it for you, you have a problem.

Q2 **What would make it turn red?**

Green with no red mirror isn't a measurement. It's decoration.

Q3 **Have you tested that scenario in practice?**

A drill. A tabletop. Not on paper.

Q4 **When did it last surprise you?**

Real measurements surprise. Quiet green for 18 months is asleep.

For red registers · Forced Prioritization: 30-day · escalation · external deadline.

PECB

INTERVENTION 05 · SPEAK THEIR STAKES

Don’t repaint the matrix. Repaint the conversation.

Counters: Curse of knowledge + Psychic numbing

FROM: *“We have a high-rated risk on supplier dependency.”*

TO: *“If our main supplier goes down tomorrow:”*

- *Day-by-day P&L impact over the next 90 days.*
- *Customer contracts we breach by week two.*
- *Regulatory questions we face by week three.*
- *Operational resilience indicators that turn red.*
- *Stakeholder confidence we lose with each press cycle.*

A matrix gets filed. A scenario gets decided.

PECB

THE FULL MANUAL

Five patterns. Five biases. Five protocols. One manual.

	PATTERN	COGNITIVE BIAS	INTERVENTION
01	Risk without an owner	*Diffusion of responsibility*	**Decide / Signs / Owns**
02	Acceptance by default	*Omission + Status quo bias*	**Make the silence sign**
03	Political cost	*Loss aversion + Self-image*	**Three scenarios, never one**
04	Drowned in the flow	*Blindness + Automation bias*	**Pressure-test + Prioritize**
05	Untranslated	*Curse of knowledge + Psychic numbing*	**Speak their stakes**

Diagnose the bias. Apply the protocol. Restore the decision.

PECB

THE NEXT MATURITY STEP

From auditor to closer.

We are trained to identify, recommend, audit. Those are the floor.

The next maturity step is closing. Engineering the decision out of the room.

WHERE DIGITAL TRUST GETS BUILT

Compliance	*proves the artefact exists.*
Digital trust	*proves the decision was made, signed, and held.*
Operational resilience	*proves those decisions hold under pressure.*
Stakeholder confidence	*is the compound interest they accrue.*

The five protocols are the operational layer underneath all four.

PECB

Next time a sound recommendation

dies without a decision.

don’t rewrite it.

Diagnose it.

Name the bias. Apply the protocol.

That’s the difference between producing reports and producing digital trust.

THANK YOU

✉ chris@cyberacademy.fr

in https://www.linkedin.com/in/christophemazzola