ISACA®
Belgium Chapter

WHY CYBER GOVERNANCE

FAILS

Even in Mature Organizations

Christophe MAZZOLA

CISO - Board Advisor - Author

Cyber Academy / Être en Cybersécurité

Lead GRC @ Cresco Cybersecurity

CISO @ Mobilexpense

Cyber Academy
Become_the_Code_Father()

Cresco.
an Integrity360 company
your security in mind

When we think about human error in cybersecurity, we always think about social engineering.

But the biggest human error is not Samantha from accounting clicking on that phishing link.

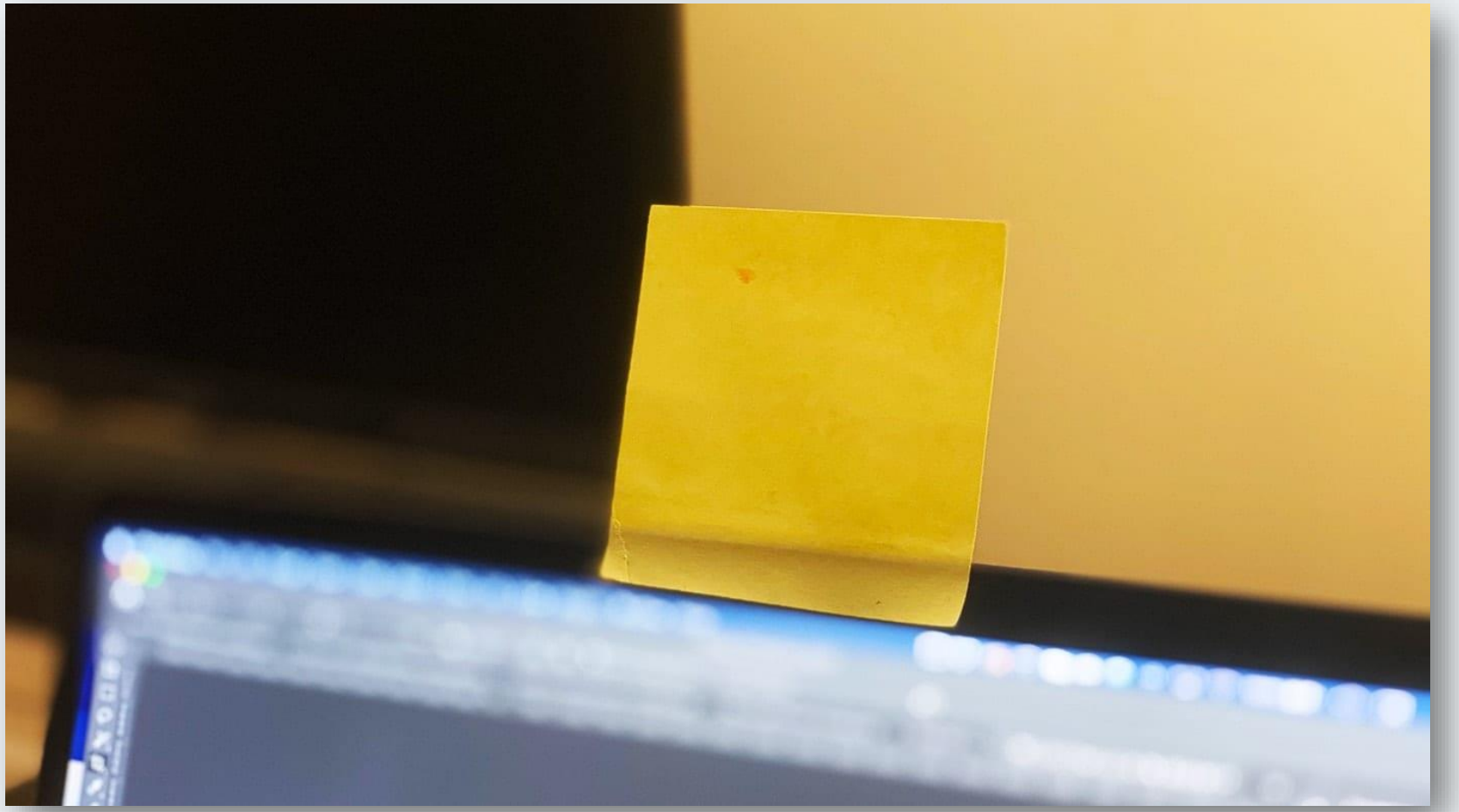
It's the human perception of cybersecurity.

Keynote by **Christophe Mazzola**


POLICIES
STANDARDS
PROCEDURES
AUDITS
TRAINING
REPORTS
COMPLIANCE
≠
VISION
STRATEGY
RISK
DECISIONS
ACCOUNTABILITY
RESILIENCE
CULTURE
OUTCOMES
GOVERNANCE
CHECKING BOXES IS NOT LEADING THE ORGANIZATION.

THE CONTROL(S)

THINK POST-IT



THE ELEPHANT

CYBER RISK IS BUSINESS RISK

The CISO’s role needs to be about enabling the business and, on rare occasions, stopping it from making a serious mistake

Christophe Mazzola

NON-NEGOTIABLES

1. Co-design, don't dictate
2. Time the Friction
3. Reset the COMEX opener
4. Workshop on Risk Management
5. Named decisions, dated decisions, signed decisions

YOU SHOULD ACT

Knowing your risk and deciding to act are two completely different things

“If we test it and it doesn’t work,

then we have a problem.”

A CISO without a seat
at the table writes reports
nobody reads.

→ Same stories
Again & Again (& Again).

NON-NEGOTIABLES

1. Calendar the decision, not the report
2. Test what scares you, not reassures you
3. A CISO without a seat is a CISO without a job
4. Audit the decision, not the document
5. Expect the unexpected

ALL ABOUT THAT GREEN

1.48%

My phishing failure rate. 12 months. continuous testing.

12%

Same people. Same month. Different simulator.

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

Green metrics can describe activity, not resilience.

217 approvals.
Not one denial.

that's not access control. that's theatre.

The 4-Question Pressure Test

1. Who chose this metric?
2. What would make it turn red?
3. Have you actually tested that scenario?
4. When was the last time this metric surprised you?

— politely paranoid, operationalised

Metrics are not the end

That’s the opener

Metrics are a tool to initiate decisions with the board

Board Management

1. My job isn’t to turn them into experts
2. They’re not clueless about cyber security
3. I’m not here to get the maximum
4. A budget rejection isn’t the end of the story

Board Management

Translate, Don’t Teach

“My job isn’t to turn them into experts. It’s to give them the tools to decide.”

Board Management

1. **Context & key threats**
   everyone in the same film
2. **Top 5–10 business scenarios**
   impact vs current control
3. **Maturity & preparedness**
   prevention, detection, response, resilience, culture
4. **Decisions you need from them**
   validations, accepted risks, sponsorship

15 min max. A short story, not an inventory.

Board Management

OPEX vs CAPEX

P&L, treasury, investor ratios.
If you don't structure it,
the CFO will with less context.

TCO

License + integration + people
+ training + maintenance.
50k€ becomes 120k€ fast.

AVOIDED COSTS

"200k protects against a scenario
with 1–5M impact. Here's the
risk analysis behind it."

SCENARIOS

Probabilistic, not fearful.
You don't scare the room
you light up choices.

"Be as strict on what you spend as on the risks you raise."

Board Management

Three Scenarios, Never One.

MINIMUM VITAL

covers the floor

Avoids the worst.
Meets minimum regulatory.
Residual risk:
fully documented.

RECOMMENDED

your reference trajectory

Solid path,
aligned with strategy.
Residual risk:
managed.

AMBITIOUS

competitive edge

Ahead of market.
Security becomes
a differentiator.
Residual risk:
minimized.

"A budget rejection isn't the end. It's a documented decision that adjusts the risk taken."

NON-NEGOTIABLES

1. Co-design, don't dictate
2. Time the friction
3. Reset the COMEX opener
4. Workshop on Risk Management
5. Named, dated, signed decisions
6. Calendar the decision, not the report
7. Test what scares you, not reassures you
8. A CISO without a seat is a CISO without a job
9. Audit the decision, not the document
10. Expect the unexpected
11. Translate the unexpected to business scenarios.
12. Three budget scenarios, never one

Easy to do. Easy not to do.

ISACA
Belgium Chapter

Thank You

✉ chris@cyberacademy.fr

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