



Spitsen en Coaches

Soft controls: Helpen niet hinderen

Jurgen van der Vlugt, RT Zwolle 11 Feb 2026

Inhoudsopgave

- Ik en **Xebia**
- Menselijk, al te menselijk
Wat nu /
Cultuur van anderen /
Hoe dan
- Samenvattend
- NOREA Taskforce Soft Controls

Start: Ik

- Ir.drs. J. (Jurgen) van der Vlugt CISA CRISC CCX RCX exRE
- NOREA, ISACA, ISSA, PvIB, ...
- EUR, 322sqn, TUD, VU, KPMG, ABN AMRO Bank, ... ZP (ICC), ...
- Into IT sinds 1978

- Sinds 46266 (zegt Excel): Xebia
- Voor de Tech (Cloud, Data, Dev, Transformation, AI) en Security



Xebia

25 years

Shaping Tomorrow
with AI Today



Applied & GenAI

Unlock the AI-Enabled Enterprise.



Intelligent Automation

Unify, Orchestrate, & Transform
with AI-Powered Automation.



Cloud & Data Modernization

Drive Growth with a Secure and AI-
ready Digital Core.



Digital Products & Platforms

Design, Build, and Scale Smarter
with AI.

Global Workforce

Our team includes over 4,500
experts across disciplines, united by
a shared passion for technology and
impact.

4.5K+

Countries

With teams in over 16 countries, we
combine global scale with local
expertise to drive results.

16

Offices Worldwide

With 28 offices around the world,
we're close to our clients and
connected to global innovation hubs.

28

Founded

Xebia started in the Netherlands
with a vision to raise the bar in
software consulting. Today, we're a
global force in AI-driven business
transformation.

2001



Human Risk Soft controls

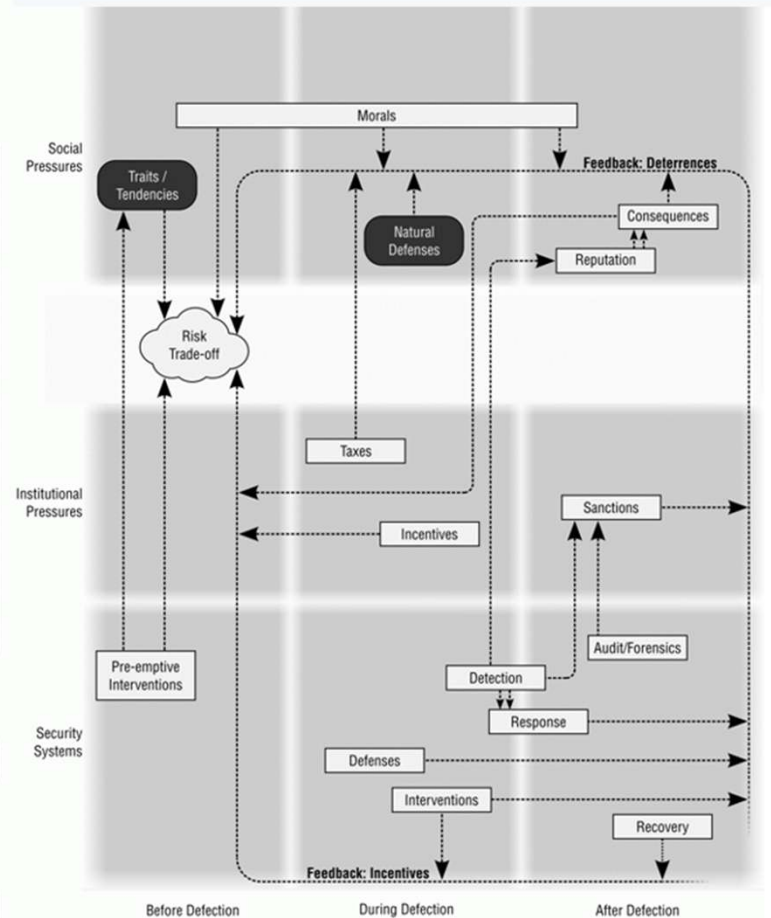
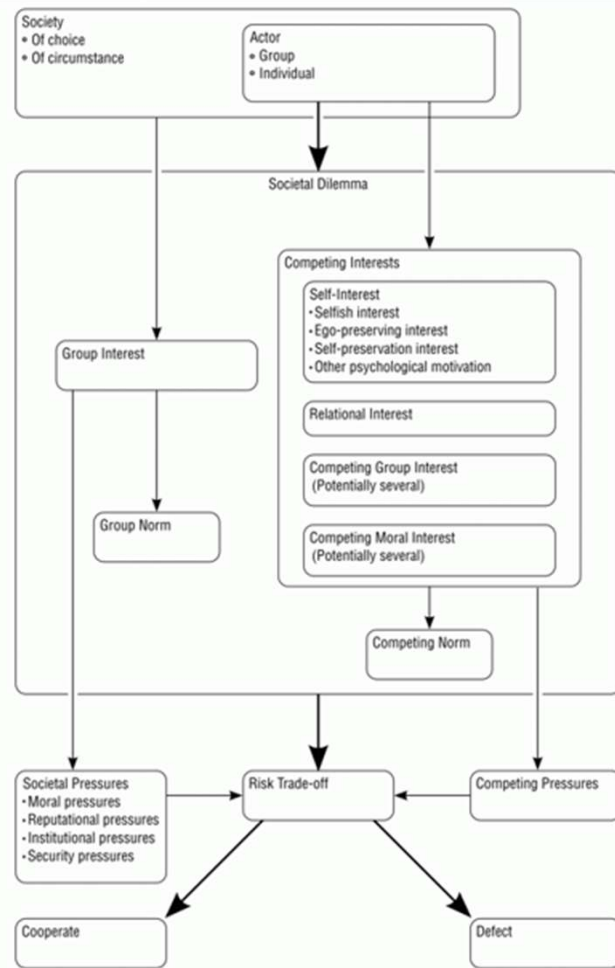
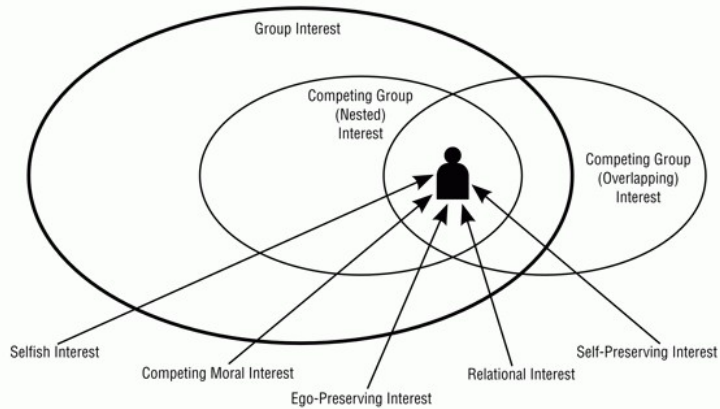
Menselijk, al te menselijk (I)

“When a human makes a mistake, the system is at fault” – Drucker

- Per ongeluk
 - Moment van onoplettendheid (vermoeidheid, geen aandacht, ...)
 - Geen zin om aandacht te geven ('mijn zorg niet', 'ze regelen het toch?')
 - Compliant gedrag is te ingewikkeld (ondanks pogingen)
- (Oh en misschien te kwader trouw)
 - Compliant gedrag is te ingewikkeld (hinderlijk / beperkend → ontwijking)
 - Motivatie-issues (ik geen bonus dan malus ik, slechte behandeling)
 - Gedwongen – dat bestaat (druk in de privésfeer / chantage / fysieke bedreiging) ...

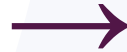
Menselijk, al te menselijk (II)

Bruce Schneier: Liars and Outliers



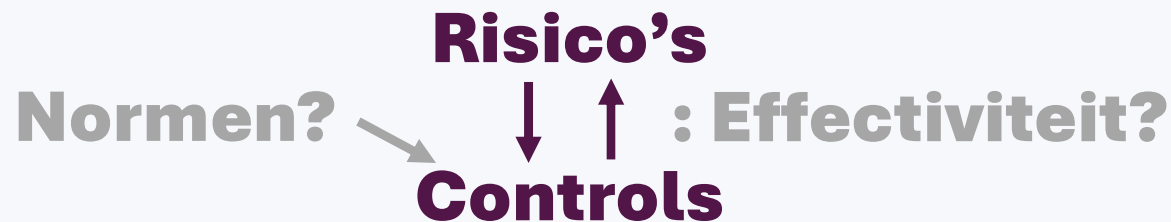
Wat nu ...

- Controls moeten sein.. ?
- Maar welke? iig *effectieve* (stop met die herhaald Bestaan = Werking onzin!)
- System is at fault én Jan Eindgebruiker (97% incl u..!) wil wél
- Maar wil vooral Performance, Velocity; Scoren en liefst nog mooi ook
- Helpen
- De makkelijkste weg is de veilige



Cultuur en indicatoren

- Kaptein e.a.: 'niet gekoppeld aan effectieve controls'
- Aardig, maar au fond niks voor de auditor (té soft; wat doet men met conclusies?)
- Aardig, maar Fancy Bear (APT28) wordt er niet braver van
- Randvoorwaardelijk, op afstand van controls
- OK, OK: Awareness > trainen; helpen = coachen
- Mits, maar, DESDA: Risk Culture (RM1 en RM2)
- Mits, maar, DESDA: Effectiviteit van Awa = betere cultuur (*vastgesteld*) ..?



- Tipje: Als Merijn Scholten in een theater in de buurt komt: Gaan!



Robert Berry • 2nd

I help auditors become awesome | Audit Trainer & Keynote Speaker | ...

1d •

I spent 3 years auditing controls that didn't matter.
They tested clean.
They looked great in reports.
But they protected very little.

At one organization early in my career,
the audit plan was full.

There was plenty of testing.
A ton of documentation.

Everything was measurable.
Everything was testable.
Everything felt safe.

The work we did passed supervisor review.
The findings were minimal.
The final reports were polished.

And yet...
nothing meaningful changed.

At the time, I didn't question it.
I thought this was what good auditing looked like.

But here's the problem.

We started with the controls.
What we didn't start with was the risk.

We didn't ask questions like:

- What could actually go wrong?
- If this failed tomorrow, would anyone care?
- What would materially change for the business if this thing didn't work?

We thought we were doing great work
by auditing "safe" and "known" controls.

Until risks popped up outside our scope.

And what about the controls
we tested so thoroughly?

They weren't broken.
They were just tied to the wrong risks.
They were guarding the wrong doors.

Here's what I learned.

1. Controls only matter in relation to risk.
2. A well-designed control tied to the wrong risk is just busy work.
3. Testing without relevance feels productive, but it doesn't protect what actually matters.

If you've ever finished an audit and quietly wondered,
"Did this actually matter?"...
You're not alone.

Van onderen

- Top-down op basis van *risicomanagement*
- Bottom-up op basis van *effectiviteit*: Levert wat we doen, betere beveiliging op ?
- (incl Wat Hebben We Al: Het moet vanwege een norm → werd nutteloos bevonden)
- Geen deugdelijk risicomanagement (RM1) door heel de organisatie
→ compliance onmogelijk; struikelen over de eerste horde
- BTW, normcompliance als toevallige bijvangst draagt NIET bij aan de bescherming
 - SandWorm maalt niet om normen
- Knettergoeie SysAdmin >> perfect certificaat
- HR + Technologie controls als *compensatie* ..!
- En denk nog eens aan Bruce Schneier

Hoe dan?

“When a human makes a mistake, the system is at fault” – Drucker

- Per ongeluk

- Moment van onoplettendheid
- Geen zin om aandacht te geven
- Compliant gedrag is te ingewikkeld

HRM/Awa + Technologie (I)

HRM/Awa + Technologie (I)

Vangrails+ (II)

- (Oh en misschien te kwader trouw)

- Compliant gedrag is te ingewikkeld
- Motivatie-issues
- Gedwongen – dat bestaat

Vangrails+ (II)

HRM/Awa + Technologie (III)

HRM/Awa(?) + Technologie (III)

Technologie (I)

Non-compliant gedrag, onbewust

- Afwijking of anomalie → Assume error / Foutje
- Foutje → Corrigeer naar (veilige!) default; zelf-richtend schip, zelf-helend beton *
- Monitor, log, rapporteer, turf voor tijdige, vroege interventie *

* Dat kan allemaal semi- of geheel geautomatiseerd! Scripts, agents, agentic

Policy-as-Code

Xebia



Vangrails+ (II)

Zoeken naar de makkelijkere weg

- Marginale overtreding → Corrigeer naar (veilige!) default; zelf-richtend schip *
- Ontdekking → Struikeldraad- en brandmelder-controls * & KPI-verlaging (?)
- Log, rapporteer, turf * voor:
 - Nudging: hinder-verminder(en)de controls *
Ribbellijnen, verharde vluchtstrook, grasstrook, vangrails
 - Extra tooling * voor snelheidsverhoging (bredere stroken)

* Dat kan allemaal semi- of geheel geautomatiseerd! Scripts — agents — Code

Xebia



Xebia

Hardcore ↔ Technologie (III)

Bewust afwijkend gedrag

- Duidelijke overtreding → Block (detectief/correctief als het kan, preventief als het moet)
- Als het niet zo duidelijk is ook:
- Log, rapporteer, turf voor tijdige interventie * + “norm-overdragende gesprekken met HR”

Policy-as-Code

Xebia

Xebia



Resultaten

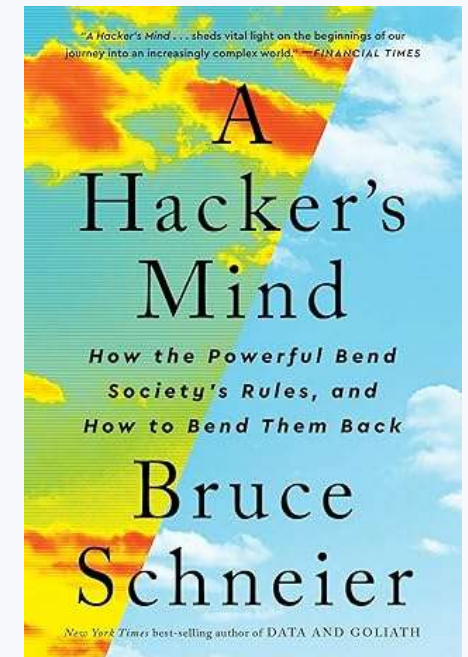
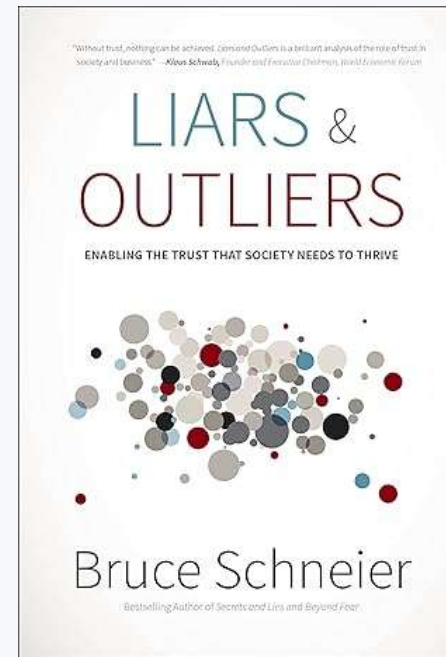
- Minder stress, minder errors & omissions, minder herstel
- Lagere kosten, hogere performance
- Versterkte cultuur (alles gaat makkelijker) , versterkte security
- Versterkte cultuur (niet gemicromanaged maar verzorgd)
- Compliance: by default ...
- Let wel:
 - Er zijn kwaaien → Afstoppen die hap; 100% harde tech inzetten
 - Er zijn risicovolle(re) situaties → Lijntjes strakker aanhalen
 - Moral hazard → ABS / 'winter'banden anyone...?
 - Defective AI
 - [Instabiele wereld → instabiele security]



Samenvattend

- Human Risk bestrijden met non-Human controls (Technologie) ... en OK, stukje HRM
- Da's 2x best soft
- Technologie $\approx$ Trad controls + "AI" inzetten: `scripts = agents - agentic` // ethisch
- Geen RM $\rightarrow$ geen zin
 - Compliance onbereikbaar
 - Nul zicht op effectiviteit, je doet maar wat
- Geen rails, maar vangrails (+)
- Voor vrijheid, motivatie en performance:
De spitsen coachen, niet voor de voeten lopen

Policy-as-Code



Clap de fin
→ NOREA



