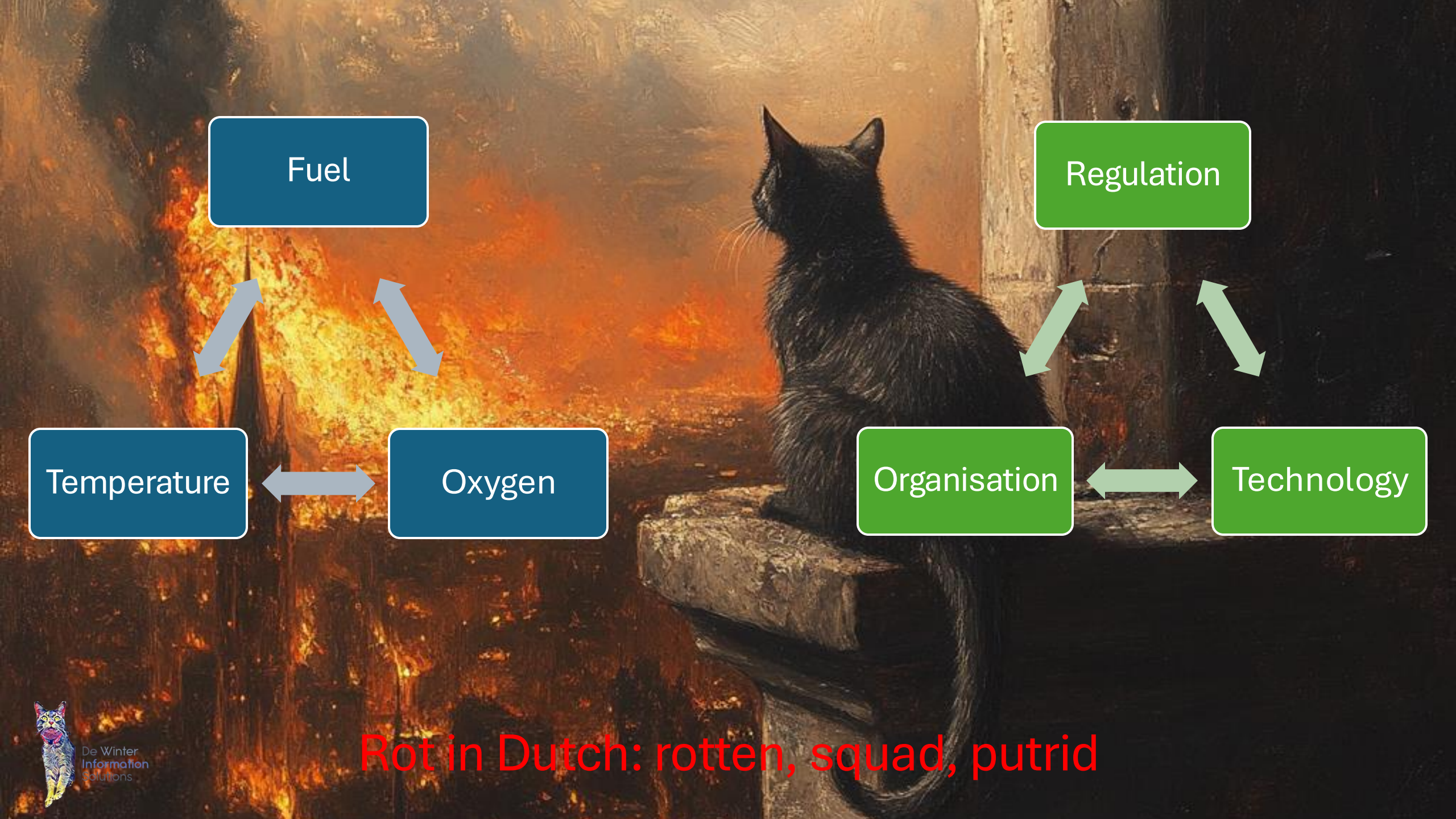
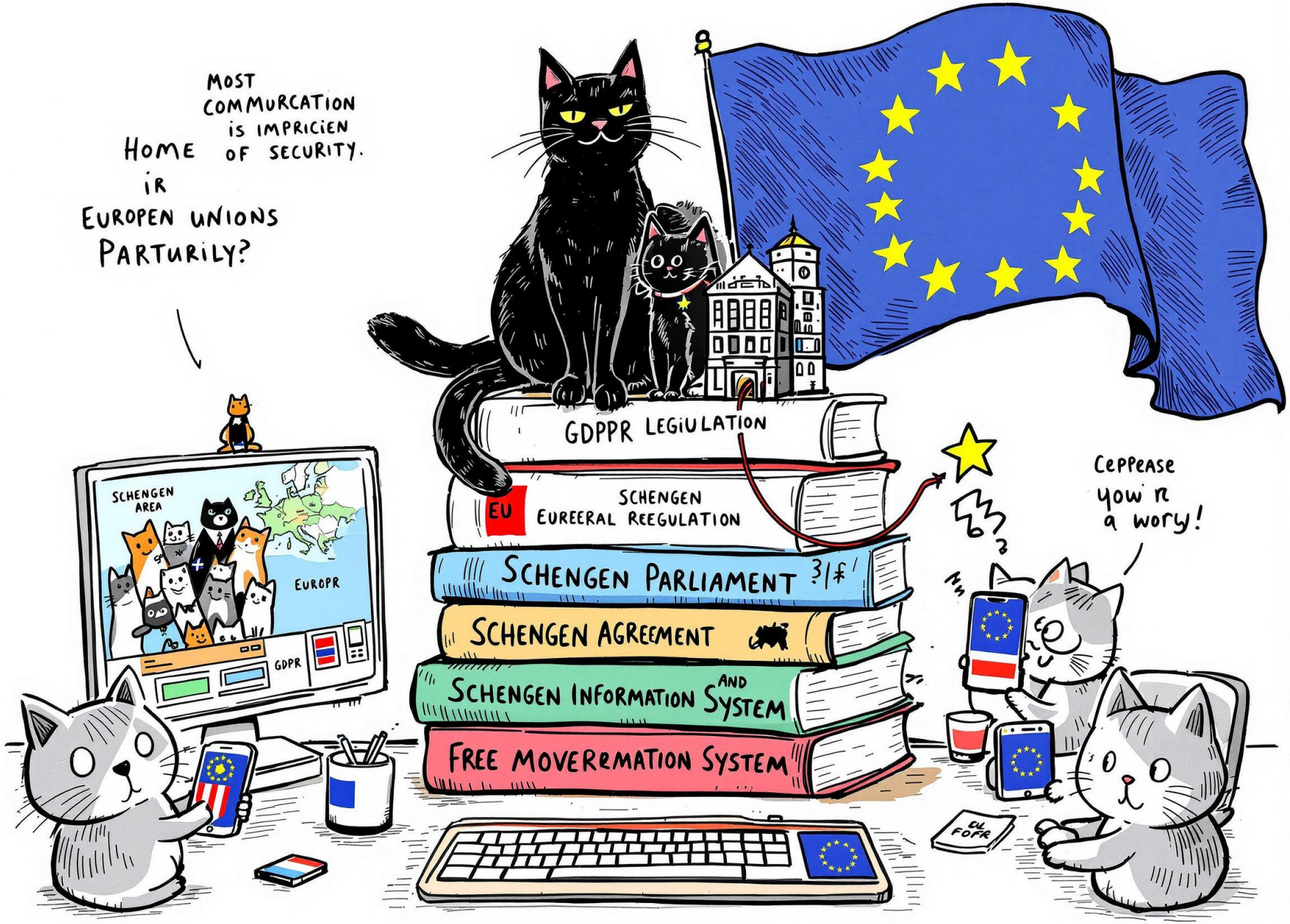
Security is ROT!

De Winter
Information
Solutions


Fuel
Temperature
Oxygen
Regulation
Organisation
Technology
De Winter
Information
Solutions
Rot in Dutch: rotten, squad, putrid

Regulation



De Winter Information Solutions

It has been chef sache all along General Data Protection Regulation (GDPR)

Article 5

*"The **controller** shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."*

Article 24

*"Taking into account the nature, scope, context, and purposes of processing [...], the **controller** shall implement appropriate technical and organizational measures to ensure and demonstrate that processing is performed in accordance with this Regulation."*

Article 32

*"Taking into account the state of the art, costs of implementation [...] the **controller** and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk."*

De Winter Information Solutions

NIS2 Directive

Article 20

*"Member States shall ensure that **members of the management** bodies of essential and important entities are required to follow training, and are **responsible** for the entity's compliance with cybersecurity risk management measures."*

De Winter Information Solutions

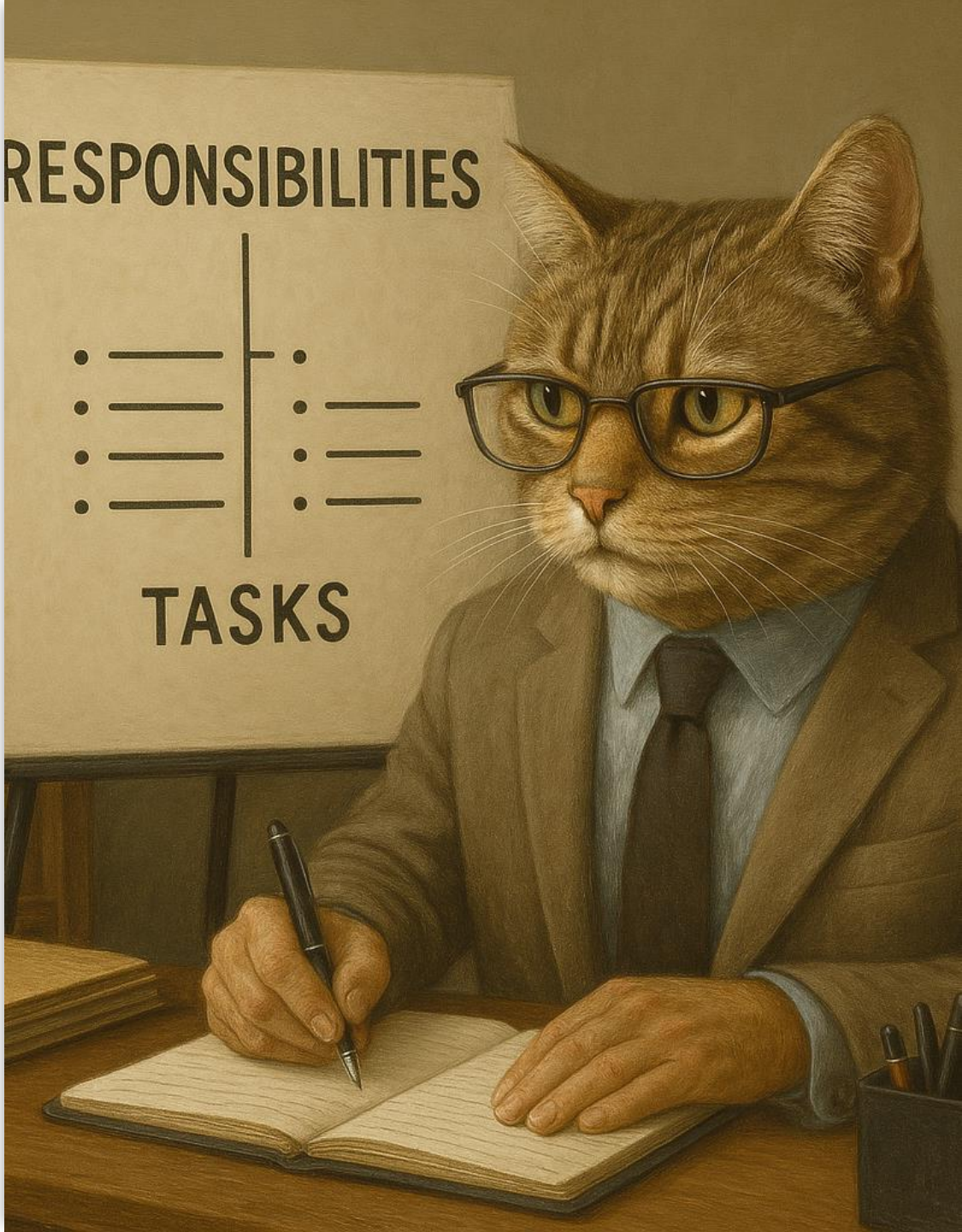
Management Responsibility

- ISO/IEC 27001 (Information Security): "Top management shall establish, implement, maintain and continually improve an ISMS…"
  - Policy, objectives, and responsibilities
- BIO (Baseline Information Security for Government): "The organization is structured to ensure information security is manageable."
  - Management must be ‘in control’
- NEN 7510 (Healthcare sector): "Management is responsible for implementing information security…"

De Winter Information Solutions

What should management do?

- Define goal
- Define and approve policies
- Determine organizational structure
  - Define roles, tasks, authorities
  - Establish governance and security ownership
- Assign responsibilities
  - Who is responsible for what?
  - Use of RACI models, job descriptions
- Monitor and improve
- Conduct reviews, audits, and evaluations
- 'Security is a management responsibility, not just an IT task.'



De Winter Information Solutions

Who's responsible?

The CEO or top executive is ultimately accountable

De Winter
Information
Solutions

Organisation

De Winter
Information
Solutions

An abritrary incident
📆 Friday

- Karel (CISO) is on a short vacation.
- Phishing incident multiple accounts compromised.
- Backup security staff unreachable; Karel joins the crisis call himself.

De Winter
Information
Solutions

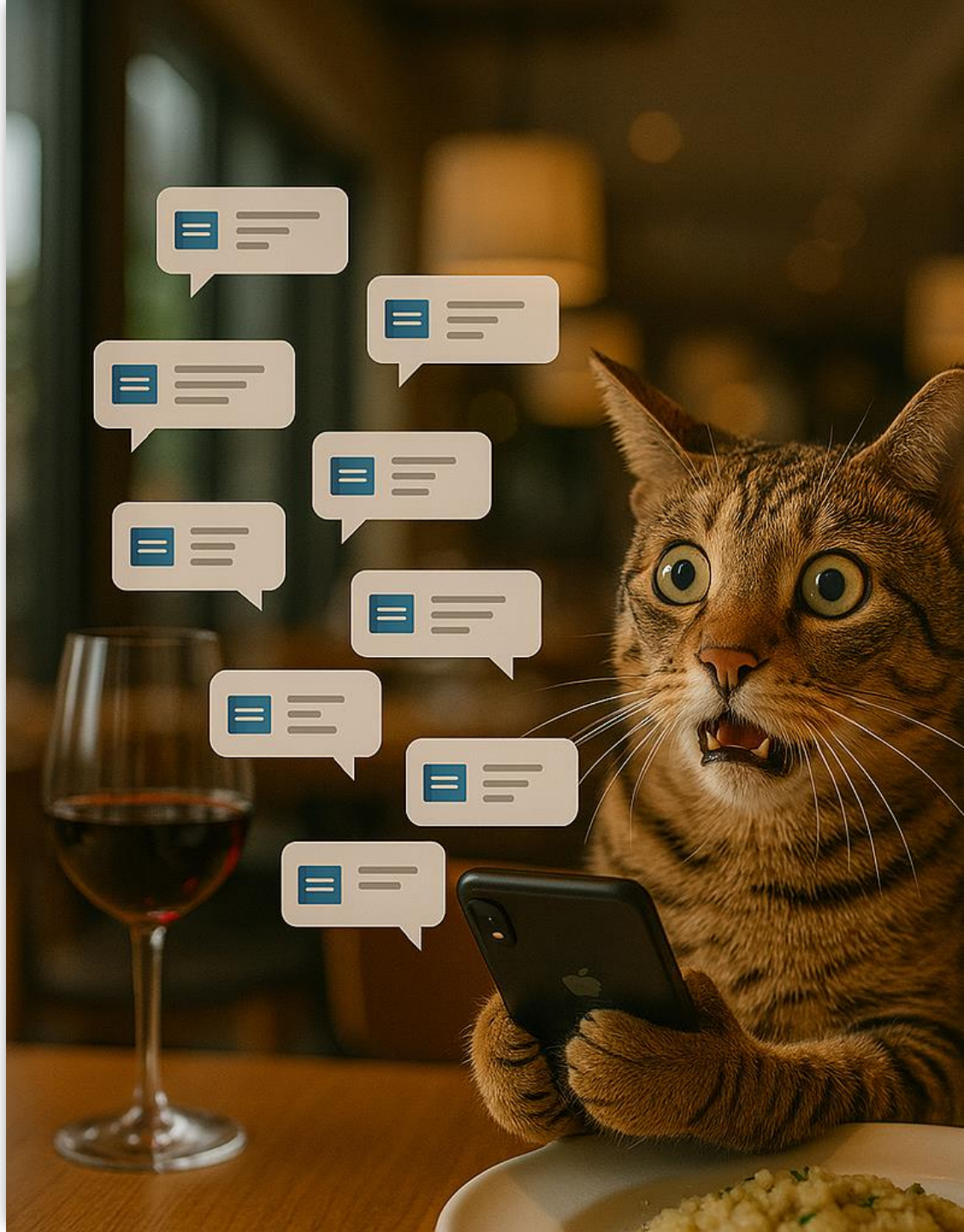
Later that day

- Anti-phishing tool was disabled months ago by an IT staffer
- Advice: reset accounts, investigate impact, inform the board.
- Business unit refuses full cooperation (“too much hassle”).

De Winter Information Solutions

A couple of hours later

- Hundreds of thousands mails sent
- Karel suggests to inform the board
- Serious damage: company domain blacklisted due to outgoing spam
- Karel acts quickly, starts getting the domain off blocklists
- Advice largely ignored; incident not reported up the chain



De Winter Information Solutions

An arbritrary incident - Sunday

- Karel receives a meeting invite from ad-interim manager
- Prepares a list of key points to clarify his actions.

De Winter
Information
Solutions

Monday – the meeting

- Manager accuses CISO of being:
  - Pushy
  - Questioned if incidents are his role
  - Not clear about the role
  - even “blackmailing”
  - Incorrect on advise. Resetting an account after several days is usefless
- Asks Karel to resign as CISO with some time to think
- Citing “health reasons” for ongoing tasks.

De Winter Information Solutions

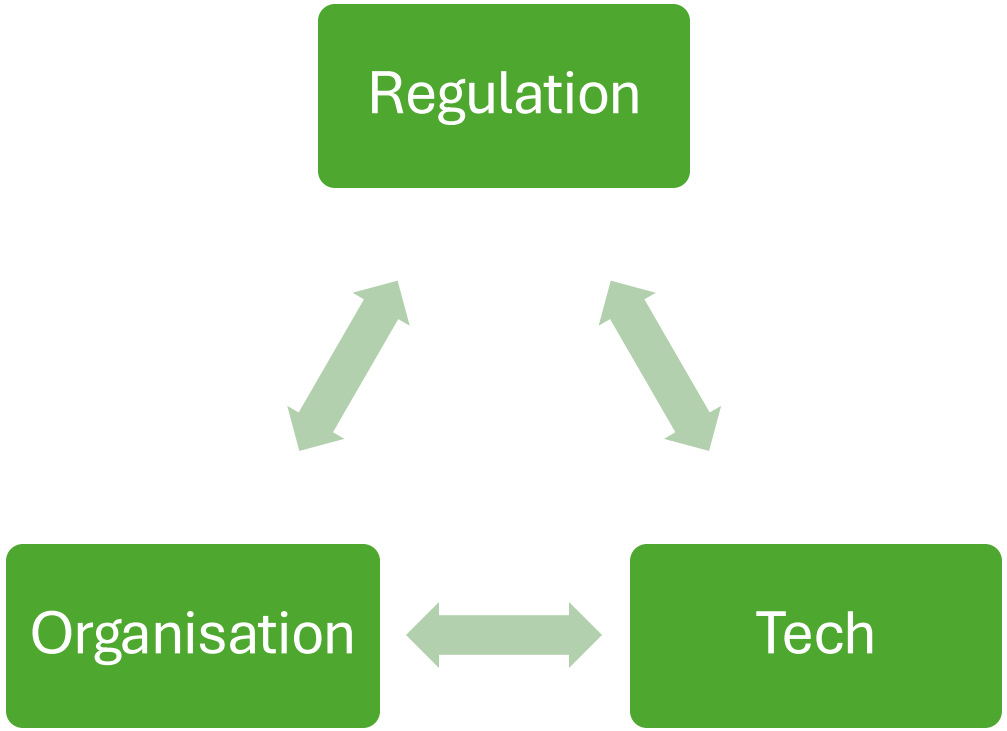
The aftermath

- Sick leave
- Legal conflict
- CISO had to leave the company

De Winter
Information
Solutions


ANALYSIS

Security triangle



De Winter
Information
Solutions

Who's responsible?

The CEO or top executive is ultimately accountable

De Winter Information Solutions

So if… if responsibilities are vague…

De Winter Information Solutions

Who are you really angry at?

De Winter
Information
Solutions

Karel was talking to a manager

- Karel wasn’t talking to the board
- There was a non-board level in between
- This led to risk filtering
- Manager was clearly incompetent on information security

De Winter
Information
Solutions


If you're not at the table, you're on the menu

Karel wasn’t a chief (as many CISO’s aren’t)

- You’re not listed in the Kamer van Koophandel as responsible
- You’re not responsible for security
- You’re not protected from getting sacked
- His lawyer used a perfect term: CISO-employee
- Don’t behave like one

De Winter Information Solutions

When you are talking to the board

De Winter Information Solutions

Karel’s safe workplace

- ✓ Role Ambiguity and Unclear Responsibilities
- ✓ Lack of Managerial Support
- ✓ Blame and Negative Organizational Culture
- ✓ Disrespect for Professional Expertise
- ✓ Negative Feedback and Workplace Intimidation
- ✓ Undermining Autonomy and Decision-making
- ✓ Stressful Environment and lack of trust

De Winter
Information
Solutions

Insecurity at work (studies)

- Lack of structure leads to insecurity about roles and responsibilities leading to miscommunication, stress and fear
- Lack of trust leads to lack of engagement, feelings of isolation and unsafety. That causes less openess, transparency.
- Lack of structure leads to more changes in the organization adding to the uncertainty.

De Winter
Information
Solutions

Cost of information security

- Dutch Cyber Security Council recommends allocating 10-20% of ICT budget
- Investment level depends on:
  - Organization's risk profile
  - Sector (Health, Financial sectors higher risk)
  - Company size (SMEs relatively higher costs)

% ICT budget	Low	Medium	High	Very High
0-5%	🔴	🔴	🔴	🔴
5-10%	🟠	🔴	🔴	🔴
10-15%	🟢	🟢	🟠	🟠
15-20%	🟢 *	🟢 *	🟢	🟠
20-25%	⚠	⚠	🟢 *	🟢

*For SMEs: at least use 'High' as a baseline.

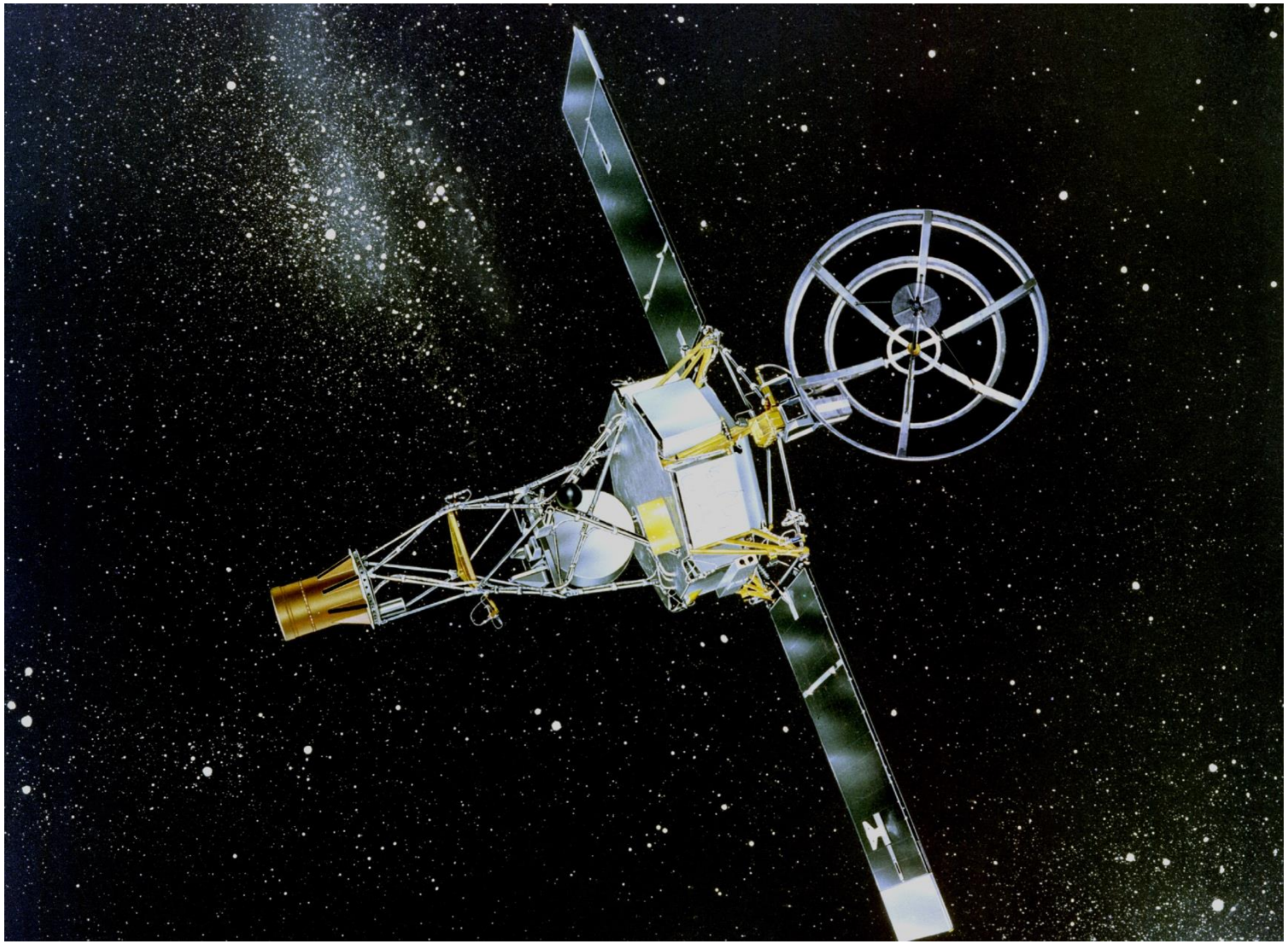
De Winter Information Solutions

Technology

De Winter
Information
Solutions

Flying past venus

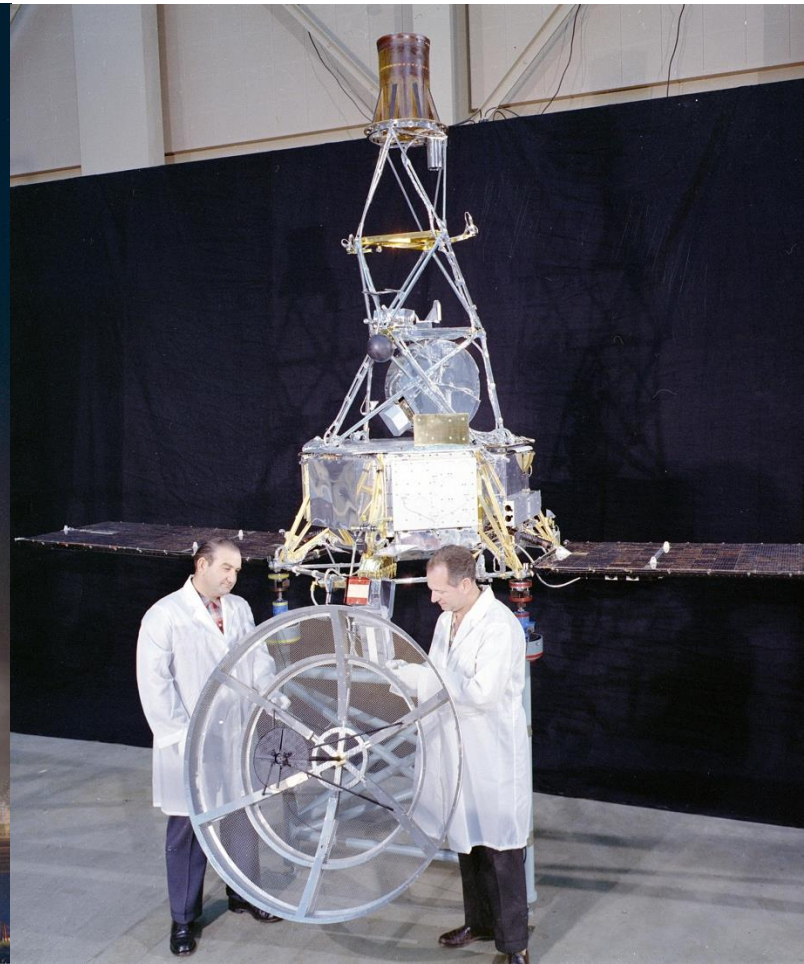
- P-37 / Mariner R-1
- 9 kilograms
- 54,000 components
- Maintain contact with Earth for 15 weeks
- Launch 22 July 1962
- Lots of toys on board:
  - Microwave Radiometer
  - Infrared Radiometer
  - Fluxgate Magnetometer
  - Cosmic Dust Detector
  - Solar Plasma Spectrometer
  - Energetic Particle Detectors
  - Ionization Chamber



De Winter
Information
Solutions

At launch

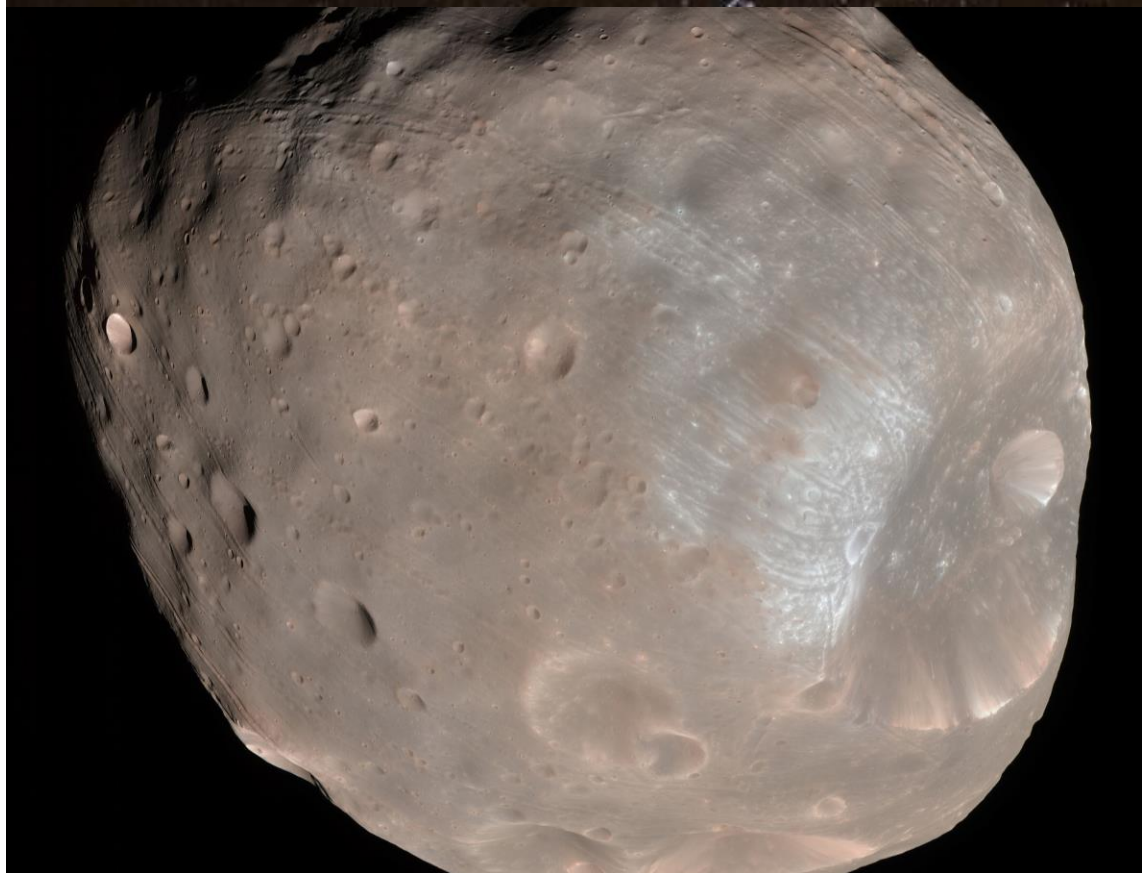
- Range Safety Officer enter self-destruct order at T+294.5 (4:54.30)
- Damage $18.5 million (now some $192 million)
- Software bug was missing: -



De Winter Information Solutions

Phobos 1

- Russian mission to view Mars and the moons Phobos and Deimos
- Journey of 200 days
- Two correction moments between days 7 and 20 and between 185 and 193.
- 2 September 1988 - no signal from the probe
- Cause a missing character: -
- A computer, which was supposed to check all commands failed
- Time pressure caused test code to remain in the system (EPROM

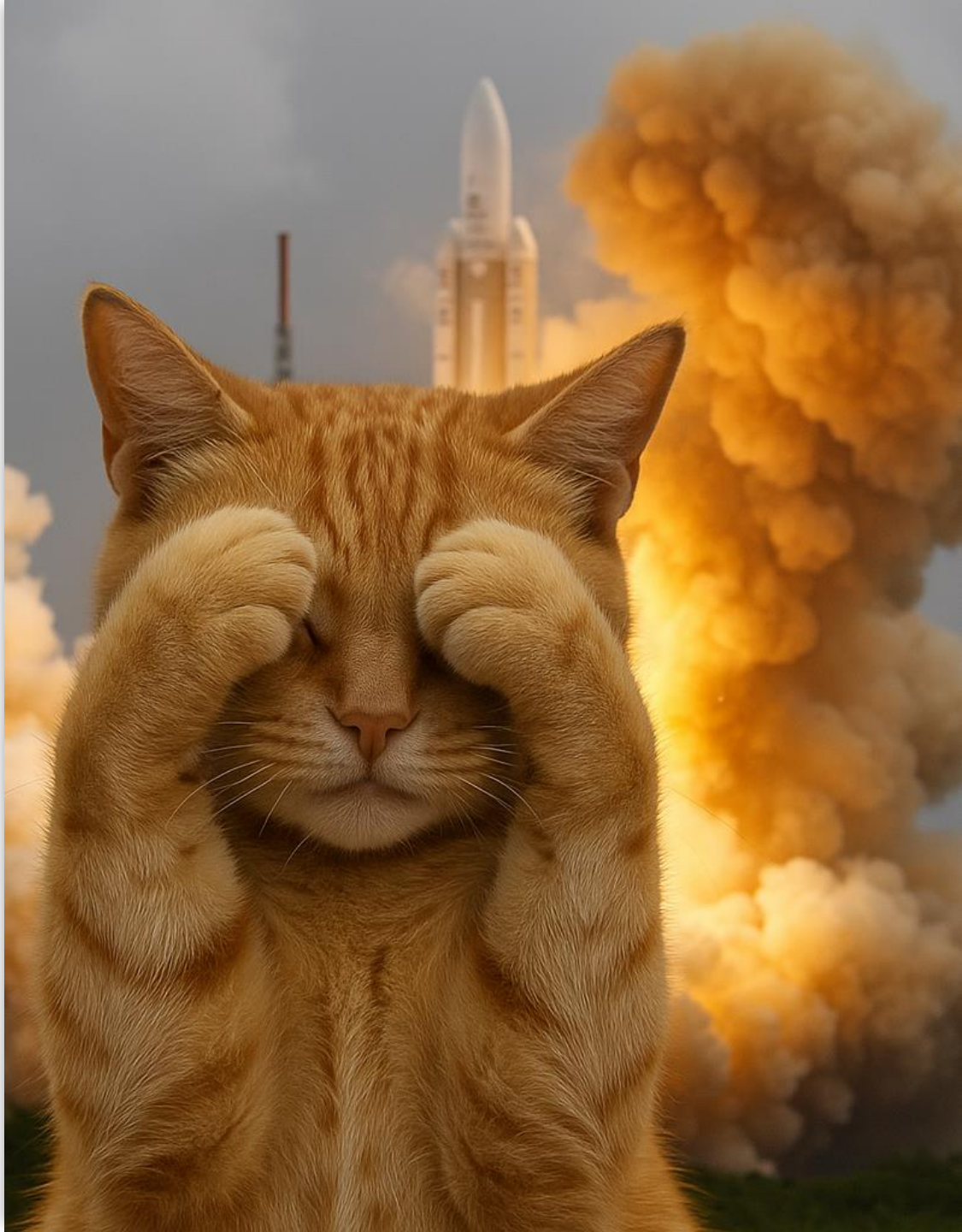


De Winter Information Solutions


June 4th 1996
Photo: ©ESA

Ariane ~~4~~ 5

- Normal behaviour 36 seconds
- Simultaneous failure of the two inertial reference systems
- Incorrect turning of the nozzles of the boosters and the Vulcain engine
- Abrupt change of course
- The self-destruction of the rocket launcher.
- The rocket software had been inherited from the Ariane 4 rocket gave erroneous signals to engines
- The software error occurred because a 64-bit floating point value was incorrectly converted to a 16-bit integer, leading to an "integer overflow"
- Damage approximately: €500 million



De Winter Information Solutions

Onvoldoende systeemtests

"The failure of Ariane 501 was caused by the complete loss of guidance and attitude information 37 seconds after start of the main engine ignition sequence (30 seconds after lift-off). This loss of information was due to **specification and design errors** in the software of the inertial reference system. The extensive reviews and tests carried out during the Ariane 5 **development programme did not include adequate analysis and testing** of the inertial reference system or of the complete flight control system, which could have detected the potential failure."

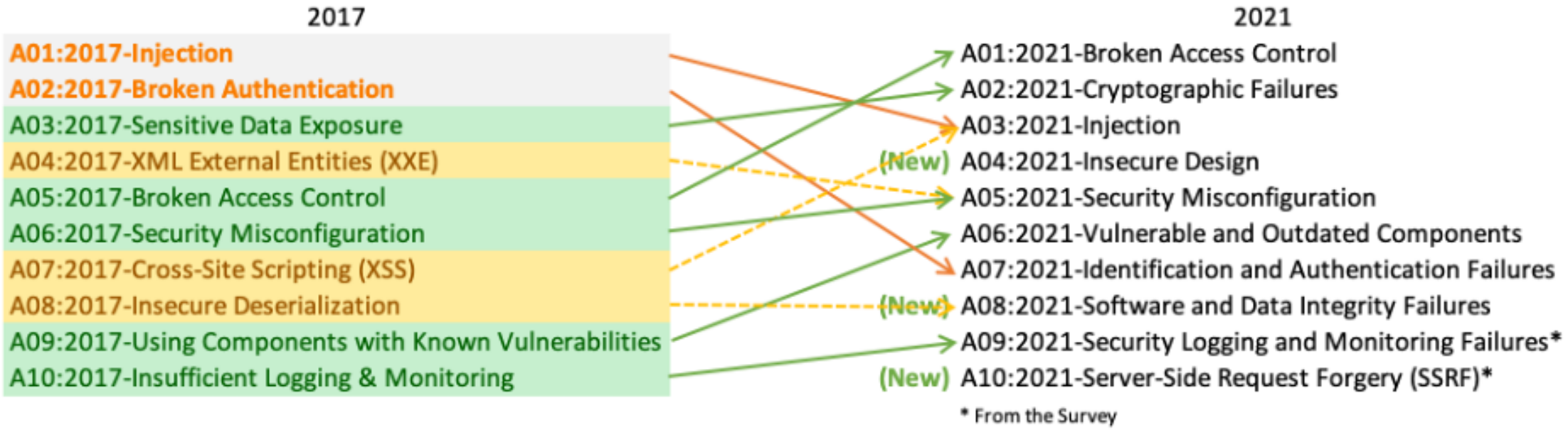
De Winter
Information
Solutions

Bad testing

- Knight Capital: In 2012, US trader Knight Capital implemented new code with a hidden flaw
- Untested old functionality was accidentally activated, causing the software to automatically buy $7 billion worth of shares in 45 minutes
- The company had to sell those positions at a huge loss (damage $440 million)
- Was fined $12 million dollars
- Cause: a simple human error during deployment and insufficient testing of the production situation

Symptoms of bad software

- Security leaks: OWASP Top 10 - the same vulnerabilities for years.
- Visual: graph of number of data breaches per year / OWASP Top 10 trends.



De Winter
Information
Solutions

Chaos Report – Standish Group

- 4 November 2024
- 50,000 projects analysed:
- 31% successful (on time, on budget, satisfactory result)
- 50% not on time, not within budget and/or not satisfactory result)
- 19% are terminated early

De Winter Information Solutions

Zibdo survey is more negative

- 31.1% of software projects are cancelled before completion
- 52.7% exceed original budget by an average of 189%
- 16.2%, of projects are delivered on time and on budget

De Winter Information Solutions

Bad software an expensive hobby

- CISQ The Cost of Poor Software Quality in the US: A 2022 Report
- By 2022 already costs $2.41 trillion (2,410,000,000,000) overall and $1.52 trillion (1,520,000,000,000)
- Losses from cybercrime due to existing software vulnerabilities soared
- Problems in the software supply chain involving underlying third-party components (especially Open Source Software, also known as OSS) have increased significantly.
- The growing impact of TD (Technical Debt) has become the biggest obstacle to making changes to existing code bases

De Winter Information Solutions

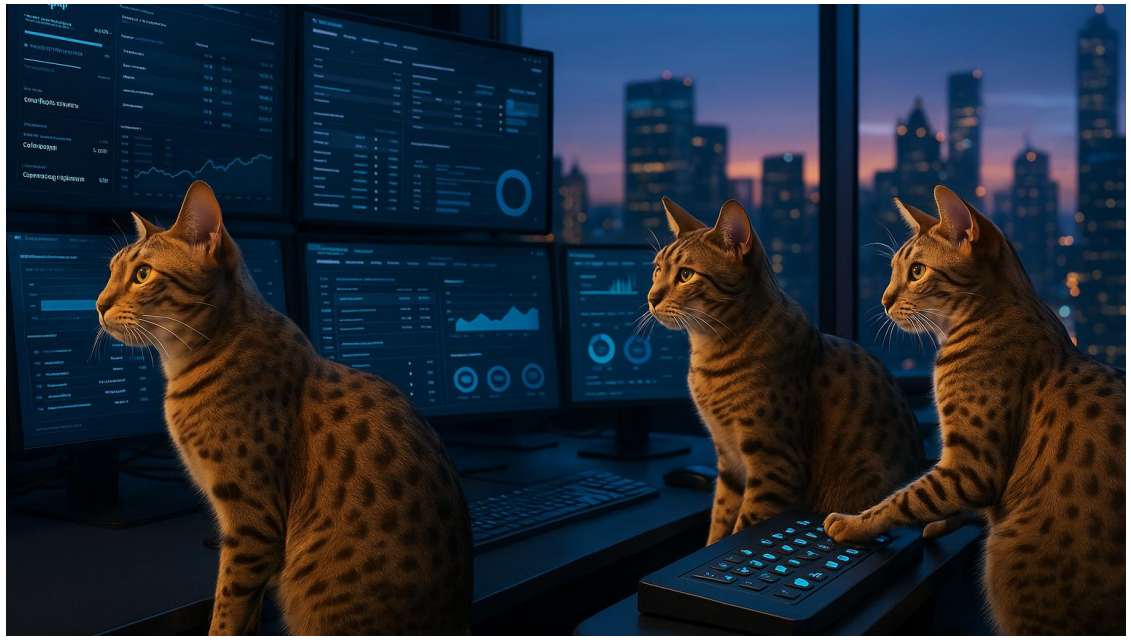
Estimate 2020

- Estimate 3 Pillar global
- $260 billion worth of failed projects cancelled
- Operational disruptions $1.56 trillion

De Winter
Information
Solutions

More than just statistics

- No more isolated incidents
- Deep-seated, systemic inefficiencies
- Significant strategic business risk
- Broad failure in planning, execution and quality assurance processes
- High rate of failure and high costs: vicious cycle?

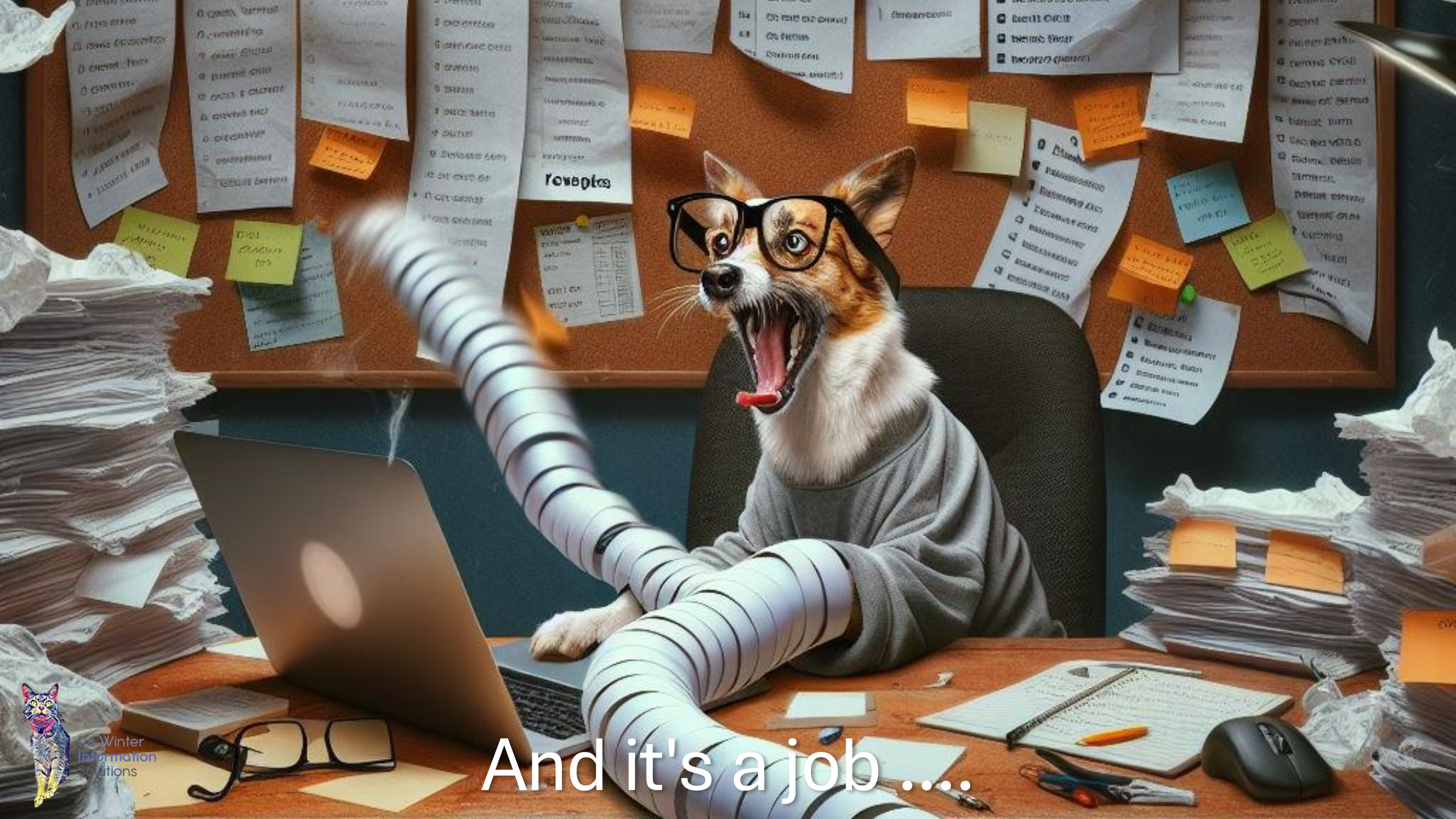


De Winter
Information
Solutions

The culture of mediocracy

- We accept the risk
- We put it on the backlog
- We accept the technical debt
- This is a non-functional
- This is a feature request
- We don't accept the bug
- 'Do we not strike out with security'

De Winter
Information
Solutions


And it's a job ....


STOP THE CULTURE
SAY NO TO MEDIOCRITY
MEDIOCRITY IS NOT
STRIVE FOR
STOP THE CULTURE OF
MEDIOCRITY IS NOT

It's just money: there will be no deaths

De Winter
Information
Solutions

De Winter
Information
Solutions

'Aviation is all about life and death'

Therac-25 (1985-1987)

- The Therac-25 was a radiation therapy machine used to treat cancer. Due to software errors, patients sometimes received extremely high doses of radiation.
- At least five patients died as a direct result of the overdoses, and several others were seriously injured.

De Winter Information Solutions

Toyota Onboard Software (2009-2010)

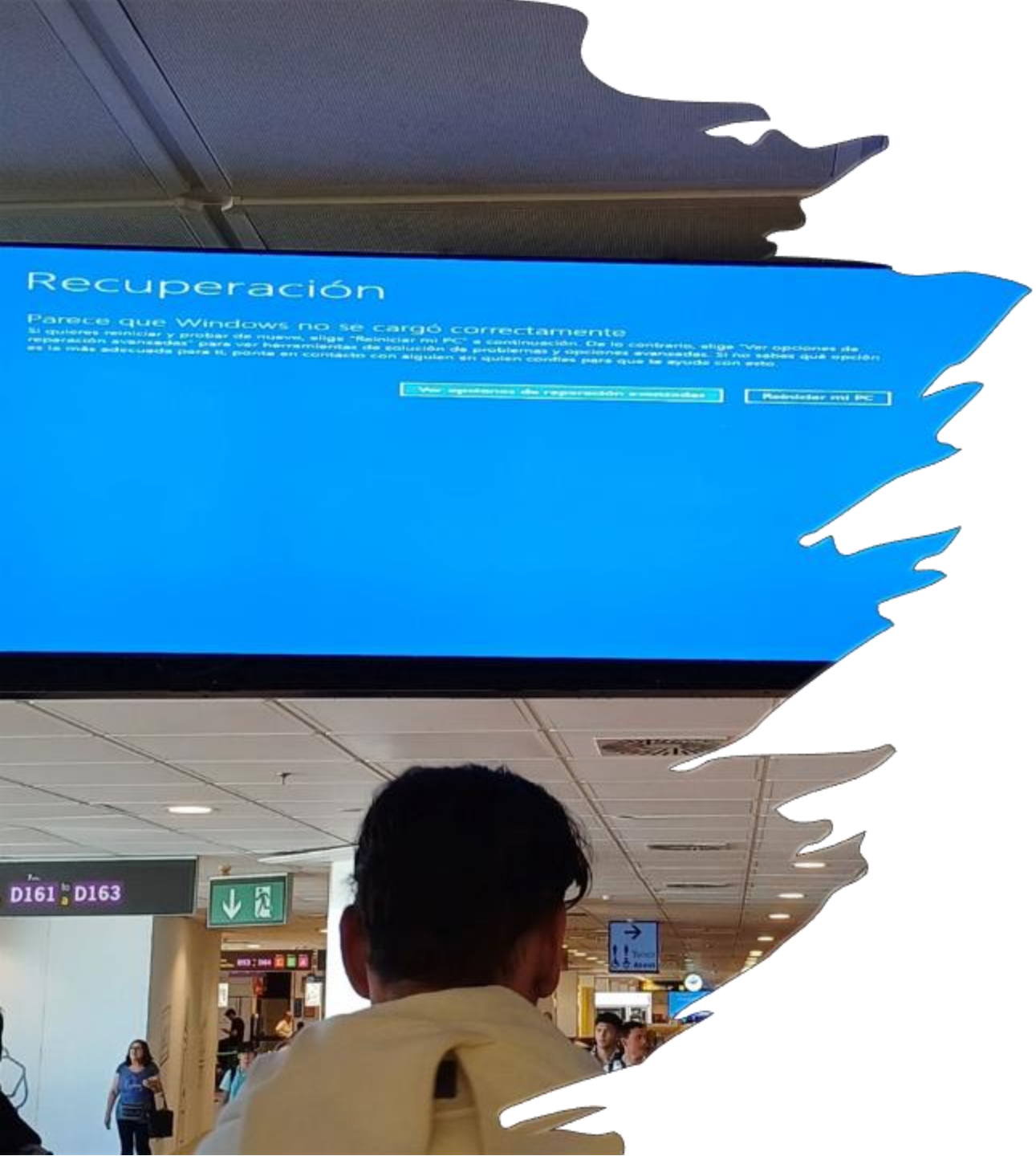
- Problems were reported with the onboard software of Toyota vehicles, leading to unintended acceleration and braking problems.
- Several fatalities were reported as a result of these software problems, although the exact number of fatalities is difficult to determine.

De Winter Information Solutions

Causes Toyota

- Spaghetti code; legacy: Unorganised, complex code ("spaghetti code") makes maintenance and debugging difficult
- No standards: Ignoring coding standards leads to many defects. (For example, Toyota did not follow voluntary MISRA-C standard and had 81,514 rule violations in the engine software. This equals thousands of potential bugs.
- Global variables chaos: Good design minimises global variables, but in bad code there are thousands of them. (Toyota's engine code had >10,000 global variables, while the academic norm is 0). This indicates lack of structure and modularity.

De Winter Information Solutions



Crowdstrike

- CrowdStrike incident:
- When CrowdStrike, a reputable security company, was itself hit by a glitch, it became clear that even the experts are vulnerable to mistakes
- Windows 10 or 11 problem
- The impact of poor validation became apparent
- Aviation example: 5,078
- Delta Air Lines claims ½ billion in damages
- CrowdStrike blames Delta's lack of security

De Winter Information Solutions

Patriot systeem (1991)

- During the Gulf War
- Due to a rounding error, a Scud missile is not intercepted during the Gulf War (timing issue)
- Dhahran, Saudi Arabia
- 28 dead

De Winter Information Solutions

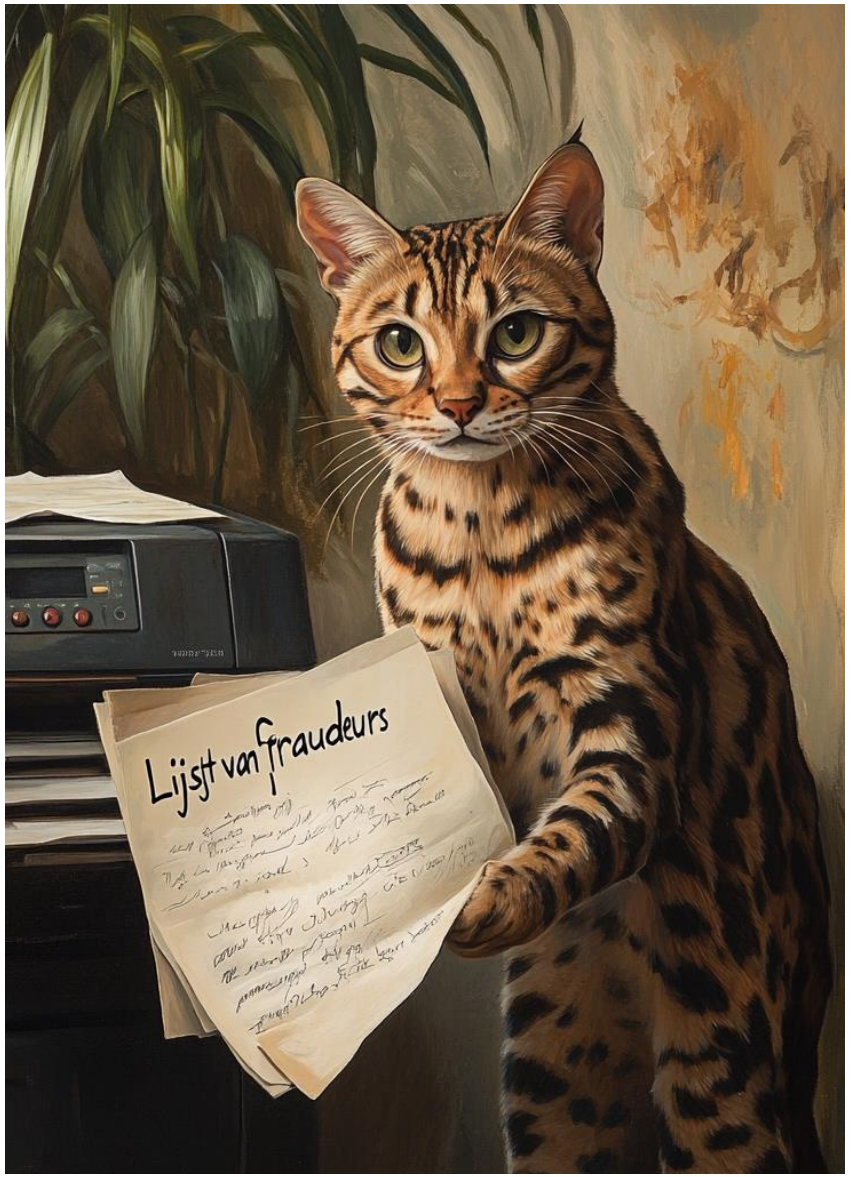
Infusion pomp

- Multiple suppliers
- Multiple software bugs
- Several deaths

De Winter
Information
Solutions

Supplements affair

- The Bulgarian fraud
- Dutch government claimed back thousands of euros in benefits from parents based on automated decisions
- There was no adequate validation of data, and human circumstances were not taken into account
- Thousands of parents were wrongly accused of fraud, leading to financial and social disruption
- Human touch and validation are often lacking in complex, automated processes, leading to serious errors



De Winter
Information
Solutions

Boeing 737 Max: flawed validation

- Remote management
- Over-reliance on Technology: Boeing introduced a new automation system (MCAS) without sufficient pilot training or thorough testing.
- Reliance on assumptions: The company assumed pilots would react quickly to system failures, but these assumptions were not validated in realistic scenarios.
- Errors in validation process: Internal reports about the system's risks were ignored. Crucial safety checks were missing in the rush to get the device to market.
- Consequences: Two fatal crashes (Lion Air and Ethiopian Airlines) and global grounding of the 737 Max, with thousands of lives affected.
- Lesson: Validation processes must be complete and impartial. Assumptions without thorough testing can have catastrophic consequences.

Failure to validate a bad and expensive joke

- Online scams in US estimated at $8.8 billion
- The Boeing affair
- Damage 737-Max affair between $20 billion and $30 billion
- Corporate recovery: $25 billion
- The benefits affair:
- Bulgarian fraud: up to €4 million
- Benefits affair: 14 billion in 2024 and the counter is ticking away

De Winter Information Solutions

Not learning from the past – as well

- 1991 - SAS flight 751
- Ice in the engine
- Automatic Thrust Restoration-system

De Winter Information Solutions

Techno-optimism

- This time we do make a perfect piece of software
- Belief in Unlimited Potential: Techno-optimism refers to the belief that technology can solve most, if not all, of humanity's problems
- No regard for risks
- Overturning critical voices
- Reduced sense of reality

De Winter Information Solutions

Interplay of multiple causes

- Poor requirements lead to poor design/logic
- Poor collaboration leads to incomplete palette of requirements
- Poor consultation/collaboration leads to changing requirements
- Bad designs lead to bad code
- Unrealistic timelines lead to shortcuts and: bad code
- Tight timelines lead: to less testing
- Cutting corners leads to backlog
- Bad code leads to technical dept
- Bad code leads to security problems

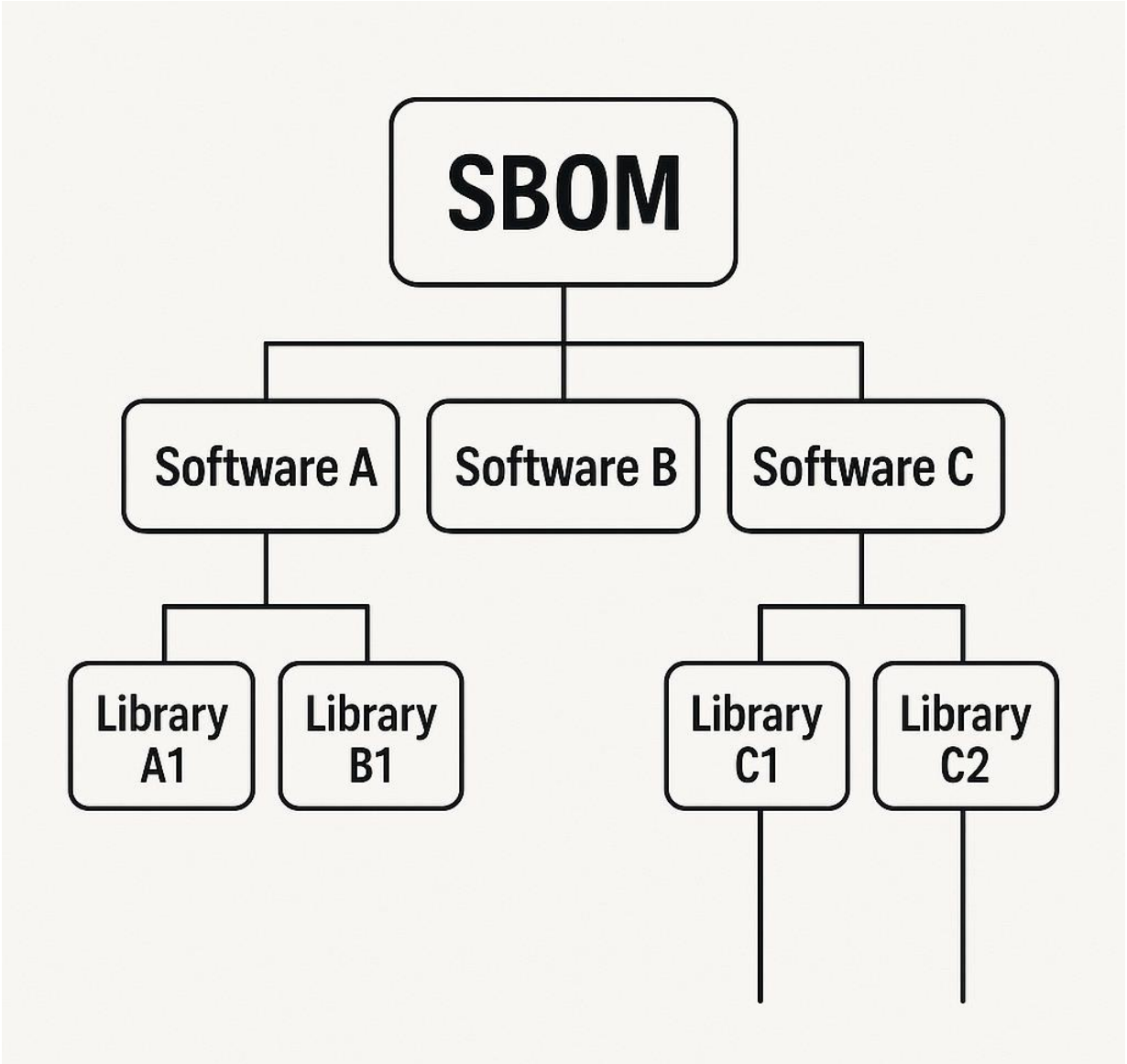
De Winter
Information
Solutions

Causes - Maintenance is forgotten

- Software is seen as 'finished'
- Legacy systems without ownership.
- Example: COBOL systems in banks and governments

De Winter
Information
Solutions

We rely on each other's software



De Winter
Information
Solutions

Falen: next level – Vibe coding

1. Collect large amounts of code written under pressure
2. Feed these to an AI model for training
3. Appoint people to interact with model
4. Above all, do not teach them programming
5. Choose a language that is hard to read (e.g. Perl or Javascript)
6. Choose a core business process
7. Get new software vibe coded

De Winter Information Solutions

Succesfactoren (Standish Group)

- Executive support - management supports employees emotionally and financially
- Emotional maturity - a set of behaviours that describe how employees work together
- User engagement - encouraging users to share their experiences and taking their opinions into account
- Optimisation - increasing business efficiency and optimising processes
- Skilled personnel - describes the high skill level of employees in technology and business

De Winter Information Solutions

Succesfactoren (Standish Group)

- SAME (Standard Architectural Management Environment) - een verzameling praktijken met betrekking tot softwareproductie, -implementatie en -gebruik
- Vaardige kennis van Agile - bepaalt de kennis en vaardigheden in Agile methodologie
- Bescheiden uitvoering - beschrijft processen die bestaan uit eenvoudige, geautomatiseerde elementen en beperkt gebruik van projectmanagementtools
- Projectmanagementexpertise - een set vaardigheden in projectmanagement
- Duidelijke bedrijfsdoelstellingen - het vermogen om projectdoelstellingen te begrijpen en af te stemmen op bedrijfsdoelstellingen

De Winter Information Solutions

Success factors (Standish)

- Good place. A good place is a working environment where the team works on software. It consists of a sponsor, a team and all other employees who work with them during the project. The influence of other collaborators can have a negative or positive impact on software development, so it is important to continuously update and improve the professional qualifications of collaborators.
- Good team. A good team drives the project and has the greatest impact on the final result. The sponsor motivates, guides and instructs the team. But ultimately it depends on the team whether it will be able to deliver the expected results. One of the Standish Group's recommendations is to form small teams.
- Good sponsor. The Standish Group defines a good sponsor as the heart of the project, without which it cannot exist. According to them, the most important aspect that leads to success is continuously improving a sponsor's skills so that they can effectively lead and support the team during the project. At the same time, this is the easiest part of the project to improve because each team has only one sponsor.

De Winter
Information
Solutions

Standish: Agile rocks

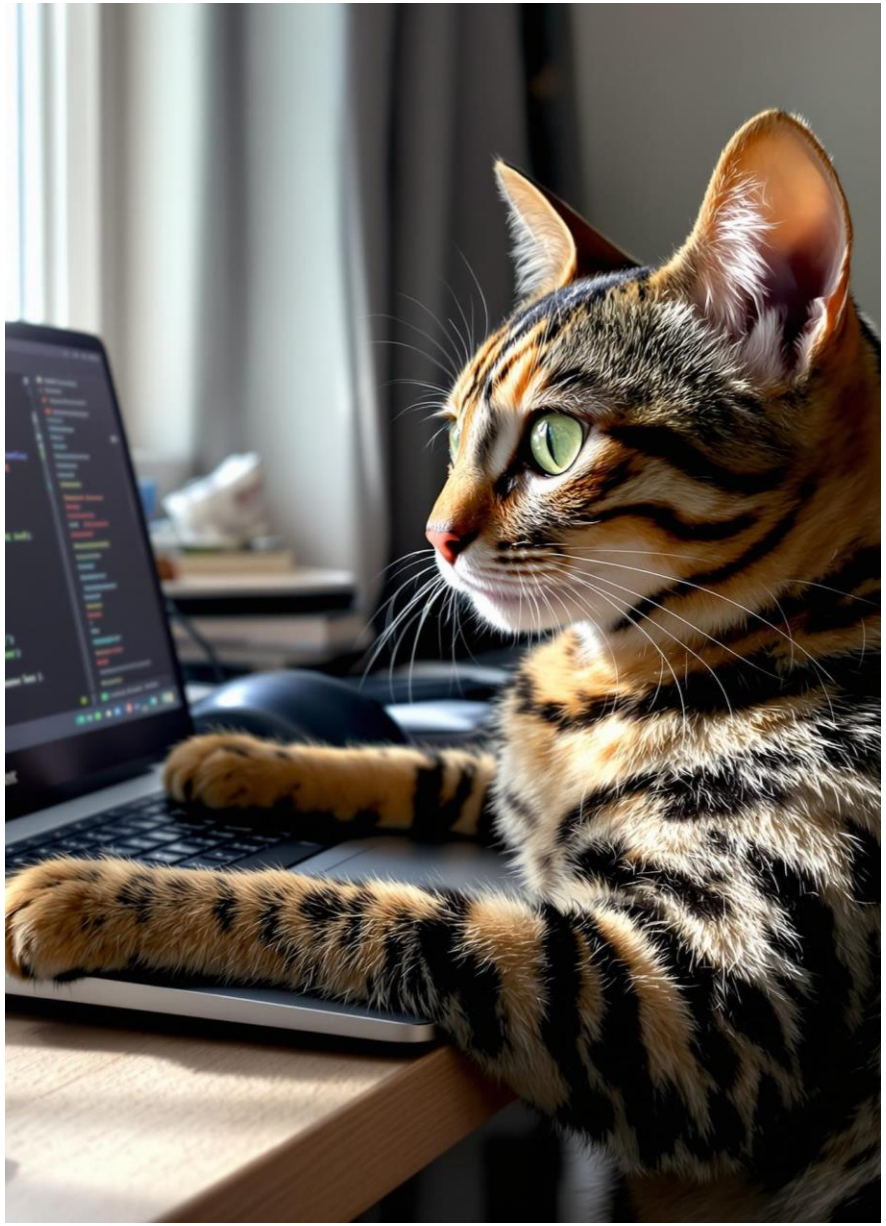
We can summarise the main recommendations as follows:

1. Teams should use the Agile methodology.
2. Instead of creating projects, we should focus on continuous and small steps.
3. We should focus on improving factors such as a good place, a good team and a good sponsor.
4. We should avoid assigning managers to projects and reduce the use of project management tools

De Winter
Information
Solutions

What else can you do?

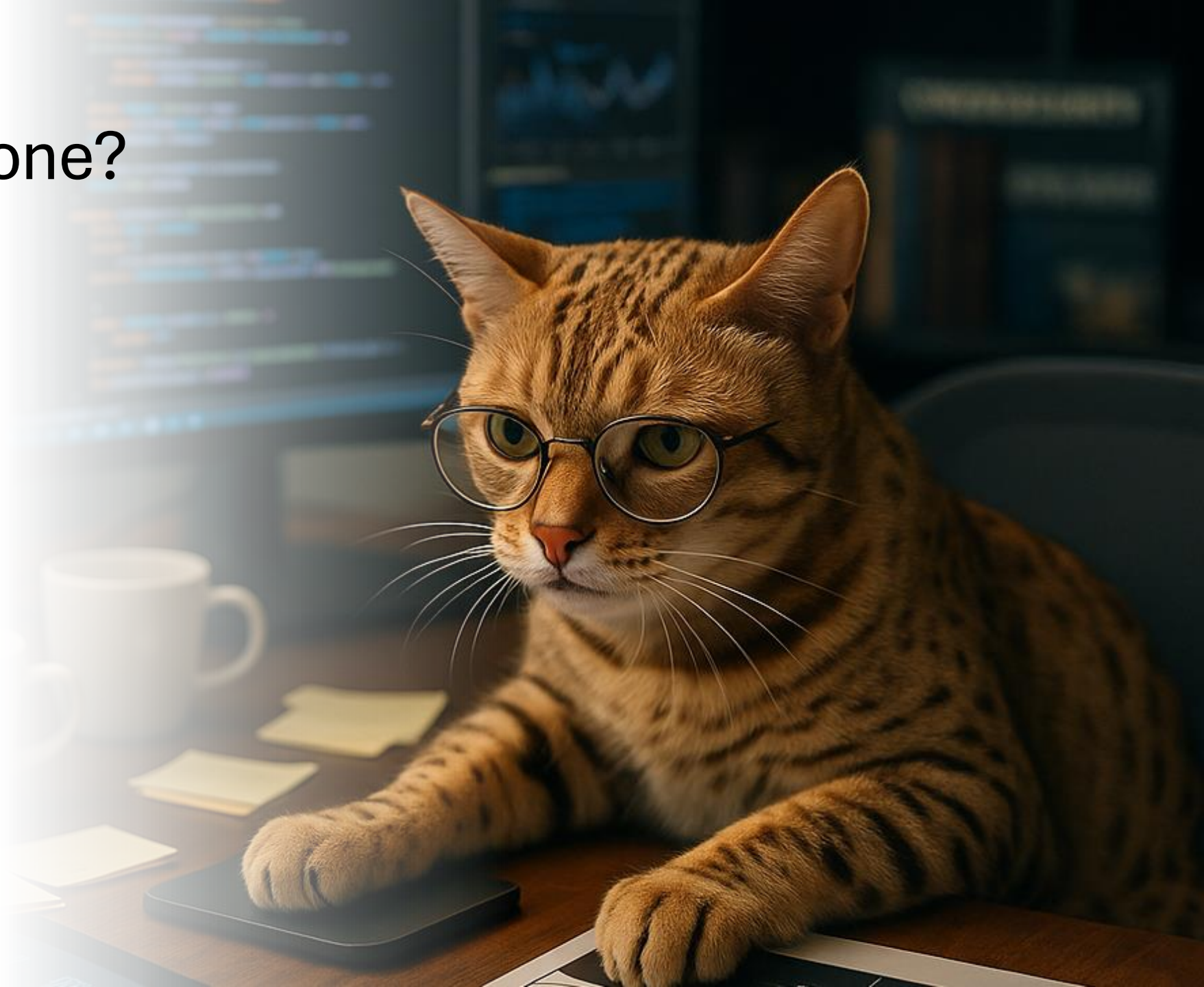
- Test culture
- Security by Design
- Testing
- Taking problems seriously
- No sixes culture
- Good CI/CD pipeline
- Focus on code quality
- Focus on security
- Sound, regular and competent training
- TESTING!



De Winter
Information
Solutions

Can it really be done?

- What sometimes there is time pressure
- You can't arrange everything



De Winter
Information
Solutions

Coronamelder: privacy first, security first

Design

- Decentralised system
- No requesting information from users
- Tight retention
- As difficult as possible to link to person
- No traceability to device
- Only necessary data
- Only transmit data after verifications
- App does not see codes

Validated

- Purpose limitation in law
- Penal provision
- No statistics party
- Cryptographically correct
- (sign everything)
- No backups
- Detecting misuse

De Winter
Information
Solutions


You can make a difference
for one goal