

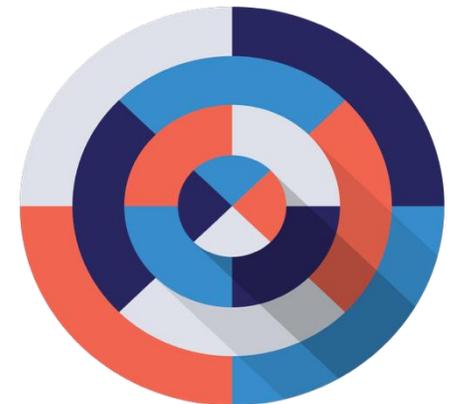
CALL IN THE CISO

3 March 2026

Edward Roozenburg
Amba Zeggen

PROBABILITY
& PARTNERS

**The upcoming threats of
Artificial Intelligence**



VSAE





You no longer need armies and missiles
to cause mass damage.



Call in the CISO Actuarial congress 2026 VSAE



VSAE

**The upcoming threats of
Artificial Intelligence**

Presenting today



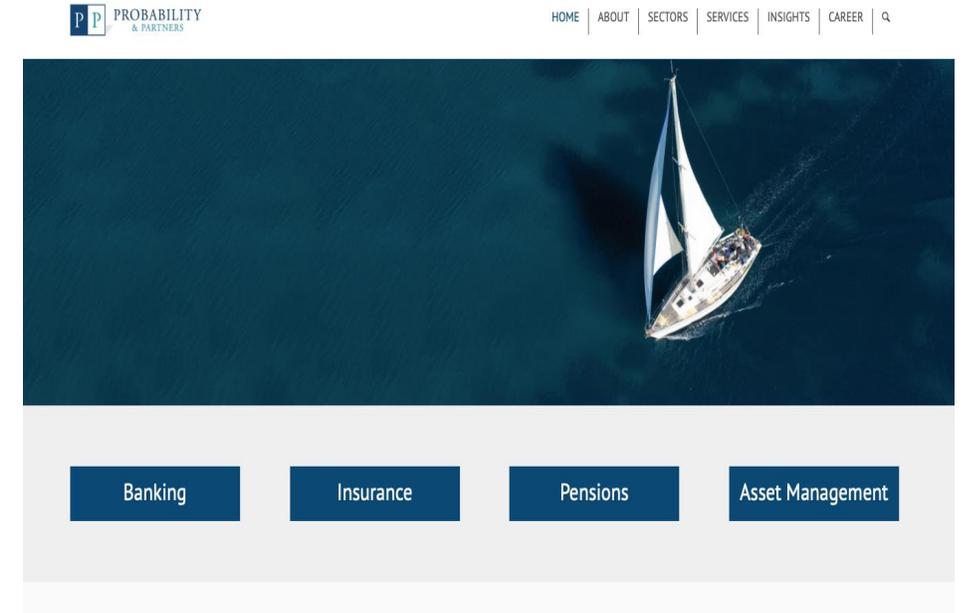
Edward Roozenburg –
edward.roozenburg@probability.nl

- Service Line Lead IT Risk bij Probability & Partners
- > 20 years of experience in audit and risk
- IT risk



Amba Zeggen –
amba.zeggen@probability.nl

- Sector Lead Insurance
- > 25 years of experience in financial sector
- Governance & Risk Management



PROBABILITY
& PARTNERS



VSAE

Story line today



The Growing Urgency of Cyber Risk



The role of the CISO



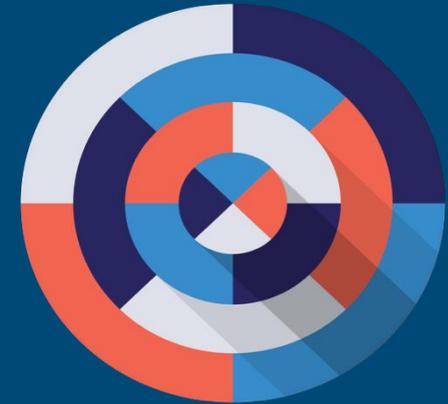
CISO & Legislation



CISO & The Actuary



Wrap-up



VSAE

**The upcoming threats of
Artificial Intelligence**



The Growing Urgency of Cyber Risk

CALL IN THE CISO

ACTUARIAL CONGRESS 2026 VSAE

The Growing Urgency of Cyber Risk

CODE



(1) Are you an Odido customer?



The Growing Urgency of Cyber Risk

1

Geopolitics

2

AI

3

Impact

4

Regulation

The Growing Urgency of Cyber Risk: Geopolitics



<https://www.cognyte.com>

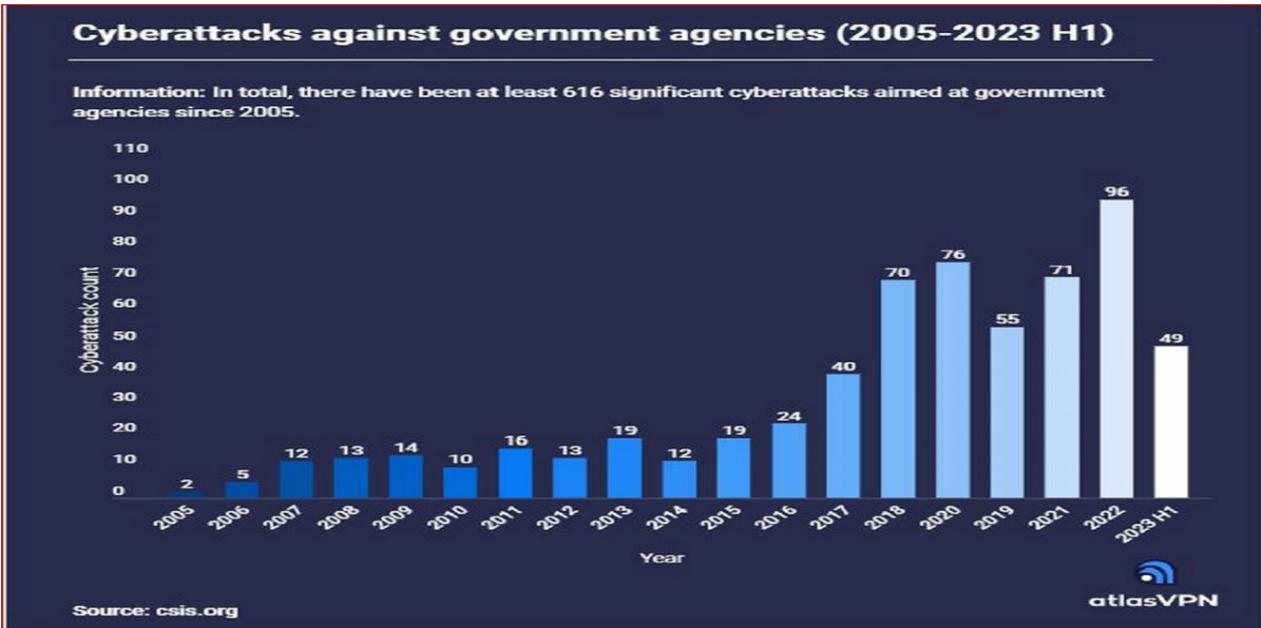
Russian hackers seized control of Norwegian dam, spy chief says

Beate Gangås says attack in April by Norway's 'dangerous neighbour' aimed to cause fear and chaos

● [Europe live - latest updates](#)



August 2025



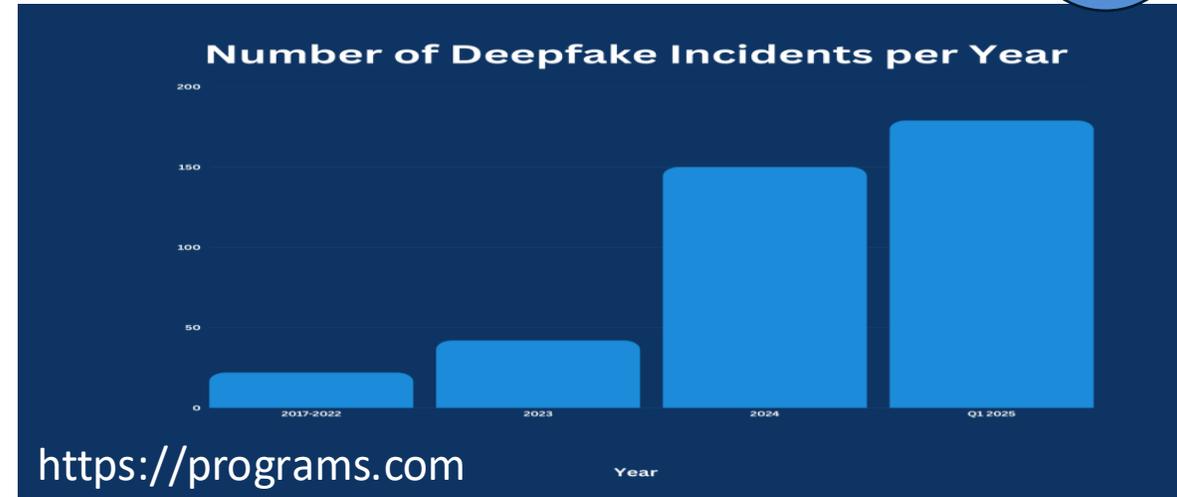
The Growing Urgency of Cyber Risk: AI

2

AI Cyber Attack Stats

- **Over 80%** of phishing emails use some form of AI.
- **87%** of organizations have been targeted by an AI cyberattack in the last year.
- Deepfake fraud attacks have risen by **over 2,000%** since 2022.
- **Around 3 in 4** AI voice scam victims have lost money as a result.
- Fully remote, scalable
- Ransomware-as-a-Service (RaaS)
- Frictionless criminal tooling
- AI lowers the barrier

<https://programs.com> and CROWDSTRIKE



The Growing Urgency of Cyber Risk: Impact

3

A single cyber event can disrupt the entire business

A single cyber incident rarely stays contained



Systems become inaccessible, dependencies ripple across the organisation, halting more and more functions

JLR cyber-attack caused UK car production to hit 70-year low for September 2023

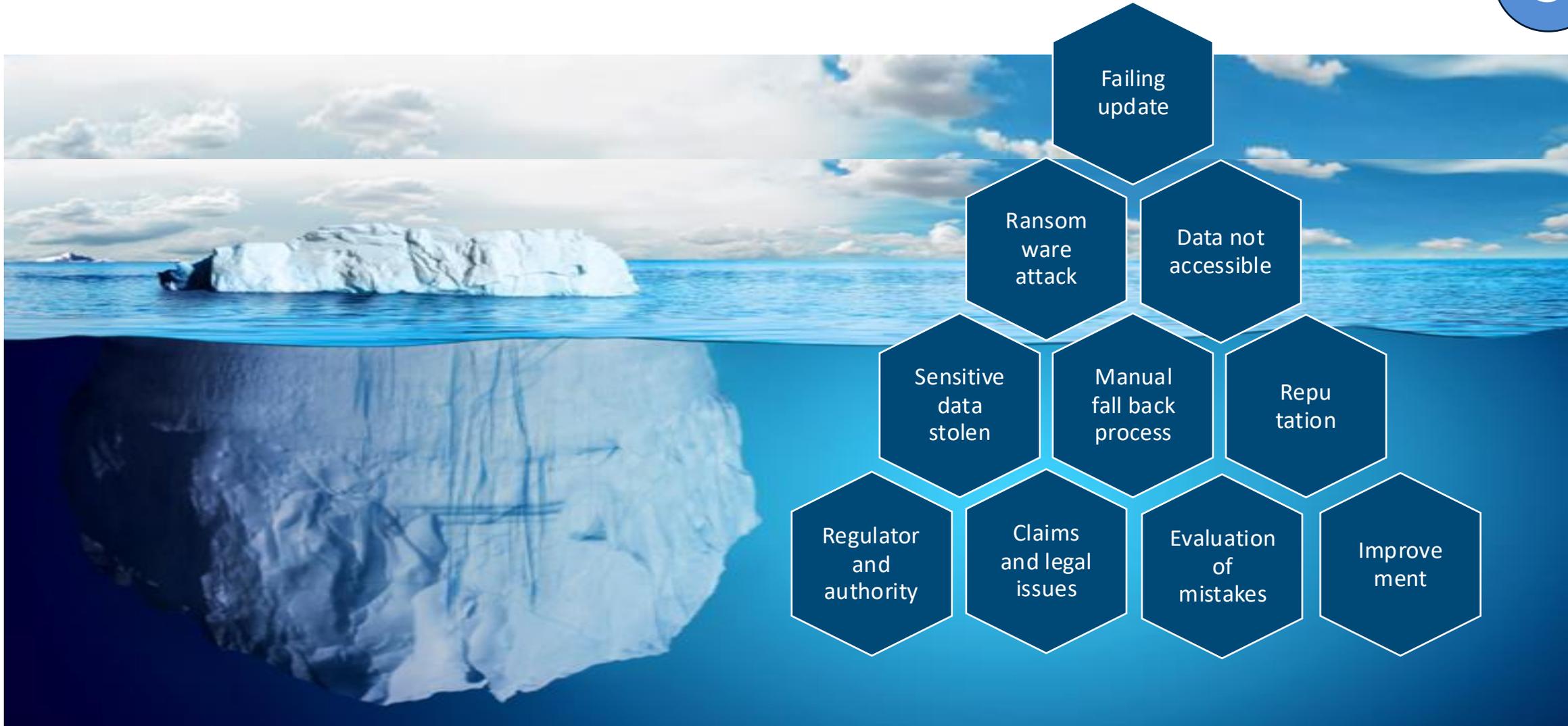
24 October 2025 Share < Save □

Josh Martin
Business reporter

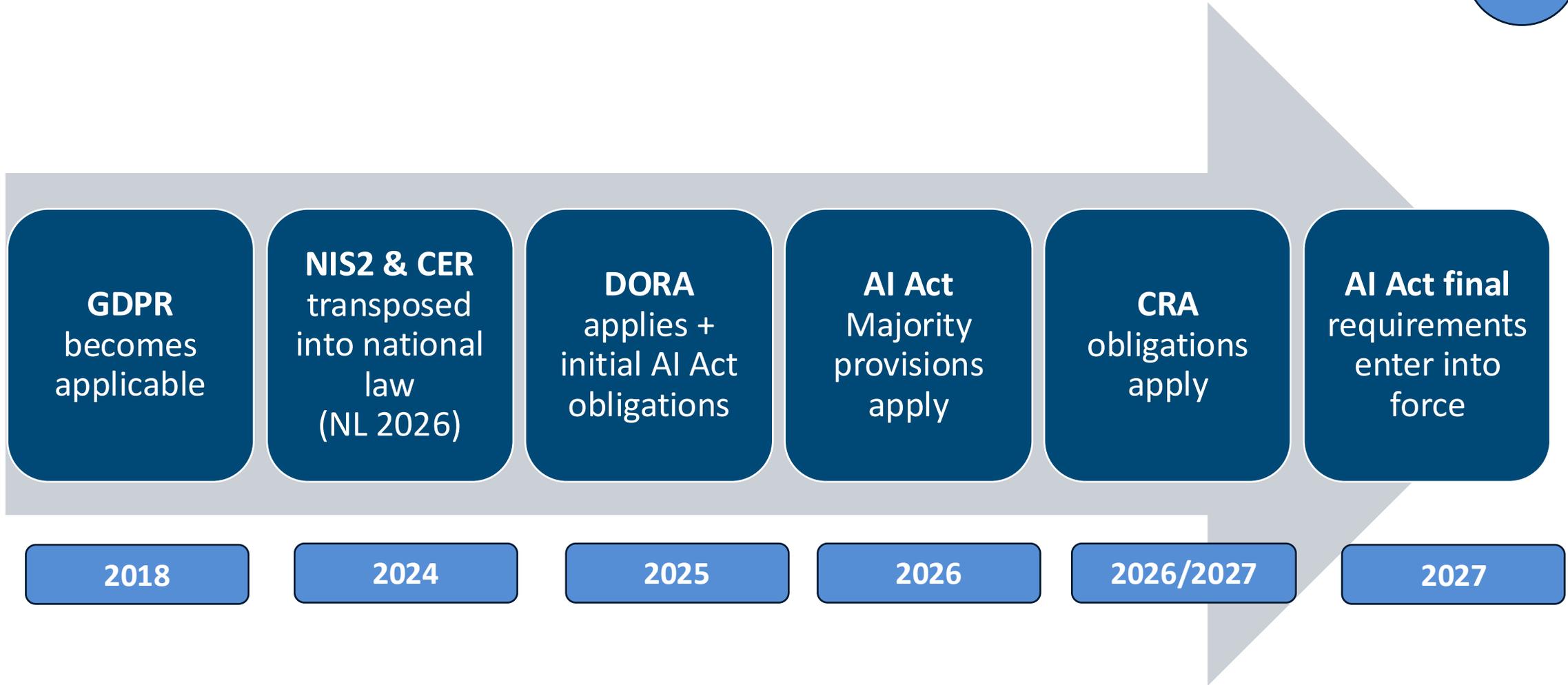


A category 3 cyber attack on Jaguar Land Rover's IT systems resulted in a five-week production shutdown, paralysing its supply chain and costing £1.9bn

The Growing Urgency of Cyber Risk: Impact - Fat tails



The Growing Urgency of Cyber Risk: Legislation





The CISO

CALL IN THE CISO

ACTUARIAL CONGRESS 2026 VSAE

The Growing Urgency of Cyber Risk

CODE

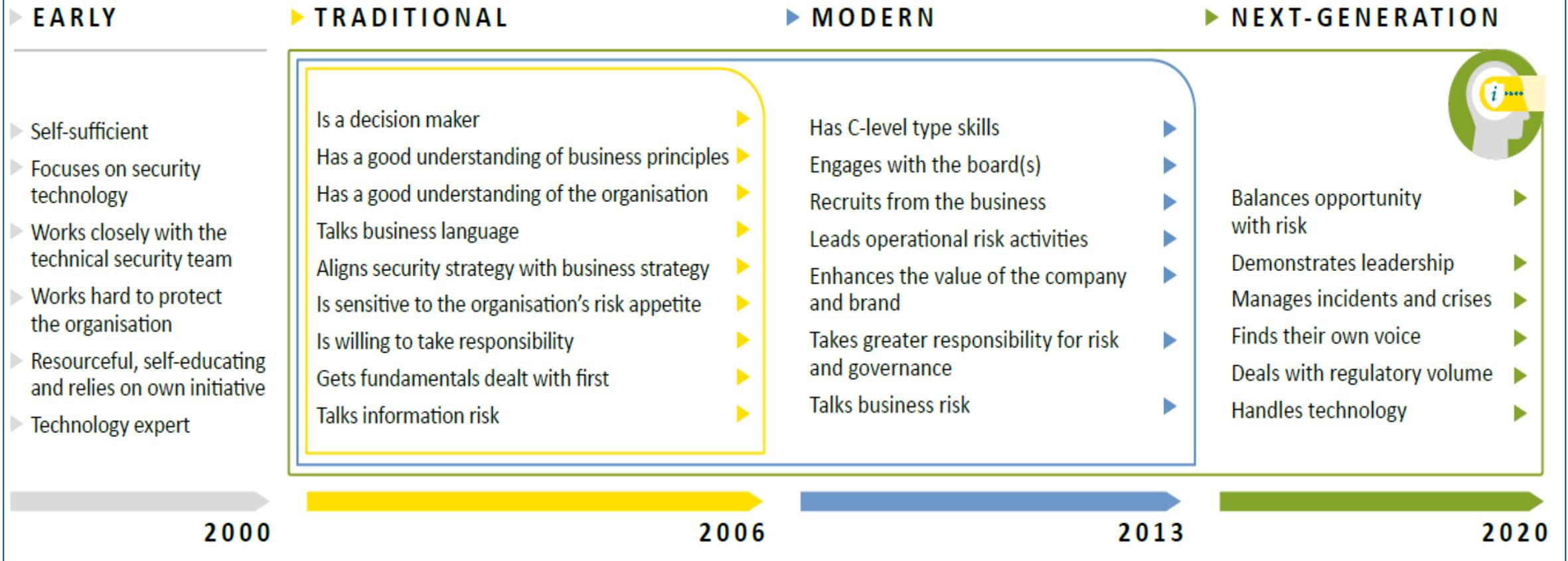
- 2) Is a CISO available in your organisation?
- a. Yes
 - b. No
 - c. What 's a CISO?
 - d. I don 't know

wooclap

Evolution of the CISO

Figure 1: How CISO skill sets have changed

ISF; becoming a next generation CISO



Role of the CISO

Strategy

Risk & Governance

Incident & Crisis

Communication & Influence

Technological insight



Strategic CISO questions



How can we accelerate AI adoption without exceeding our cyber risk appetite?

Home > Security

CrowdStrike says AI is officially supercharging cyber attacks: Average breakout times hit just 29 minutes in 2025, 65% faster than in 2024 – and some attacks take just seconds

Cyber criminals are actively exploiting AI systems and injecting malicious prompts into legitimate generative AI tools



How can we reduce the dependence on software vendors in geopolitical sensitive region?



How can we improve client trust with our new digital customer platform?



What happens during a 10-day cloud outage?

TECH GIANTS

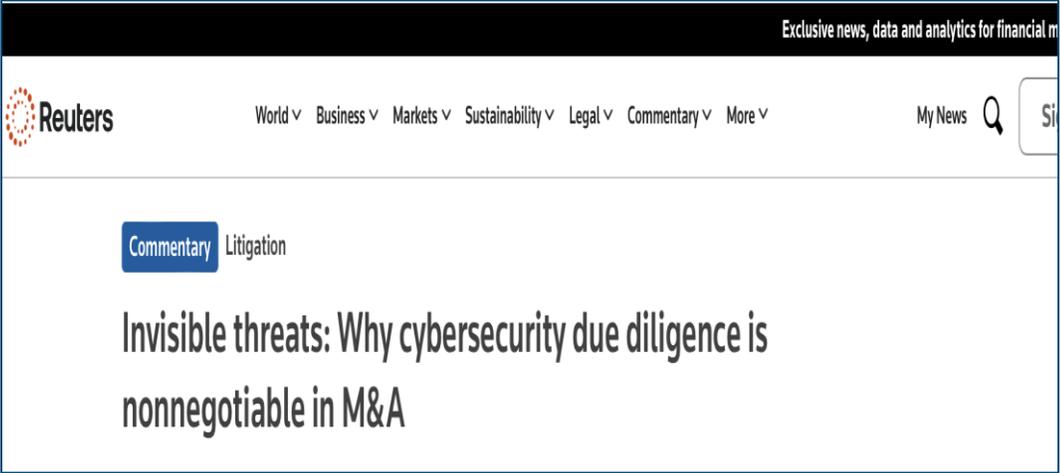
The day the cloud went out

Entrepreneurs and tech workers from around the world describe how they navigated the many cloud outages in 2025.

Strategic CISO questions



Is this acquisition safe from a cyber-risk perspective?



How resilient are our operations against geopolitical threats?



How do we ensure new digital platforms are secure-by-design without slowing down the business?



Do we need cyber insurance?



No CISO: what could go wrong?

- Security gaps are undervalued
- Security strategy is not aligned with business strategy
- Security seen as “IT only”
- Risk aversion and risk taking is not balanced

The screenshot shows a news article from CrowdStrike. On the left is a vertical banner for the '2026 Global Threat Report' with the subtitle 'Year of the Evasive Adversary' and a 'GET REPORT' button. The main article title is 'CISOs Rise to Prominence: Security Leaders Join the Executive Suite'. The sub-headline reads: 'Security professionals are moving up the executive ranks as enterprises face rising regulatory and compliance standards.' The author is Arielle Waldman, Features Writer at Dark Reading, dated January 16, 2026, with a '6 Min Read' indicator. Below the text is a photo of a diverse group of business professionals in a meeting. To the right of the photo are two 'Edge Picks' sections: 'APPLICATION SECURITY' featuring 'AI Agents in Browsers Light on Cybersecurity, Bypass Controls' and 'CYBER RISK' featuring the Adblock logo.

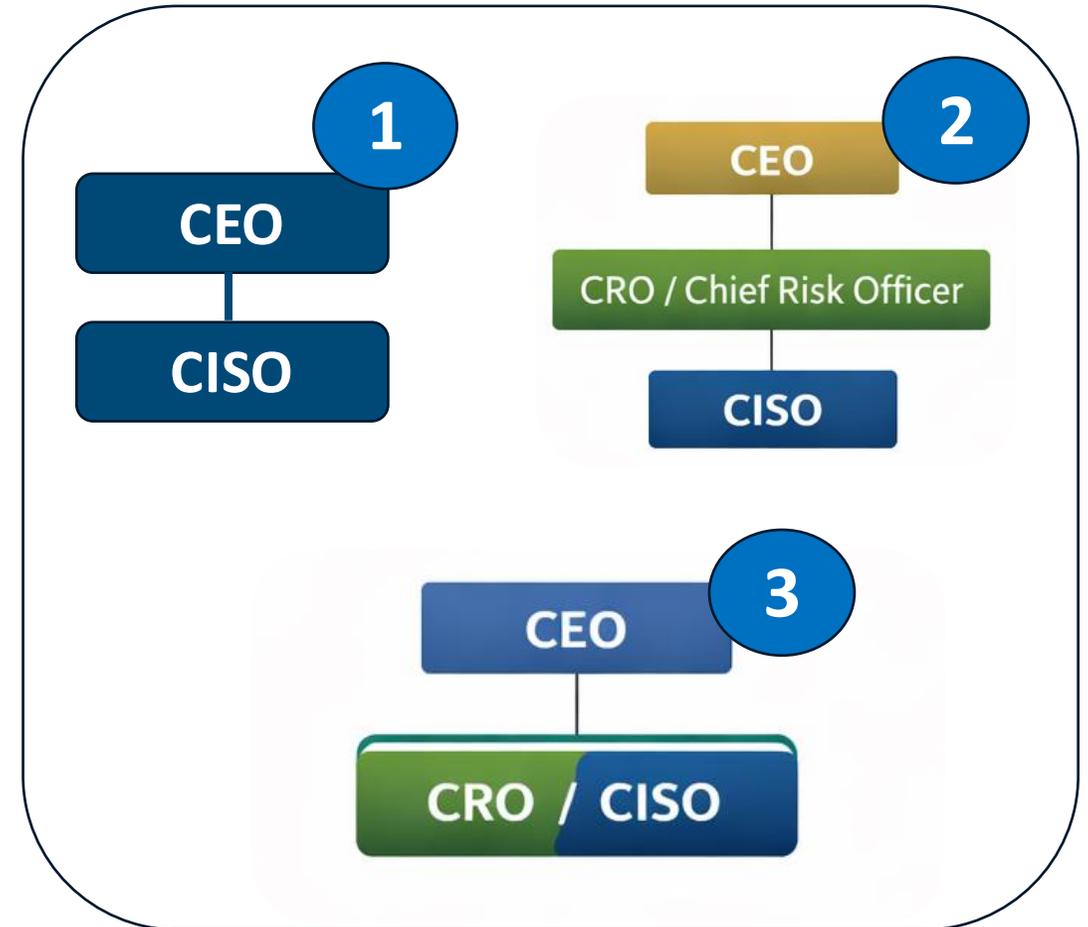
Position of the CISO

Do we need another “C”?

Direct and independent escalation rights to the board

Cyber risk is its own discipline

Part of strategic decision making



What do we see in practice?



Many organizations do not have a CISO



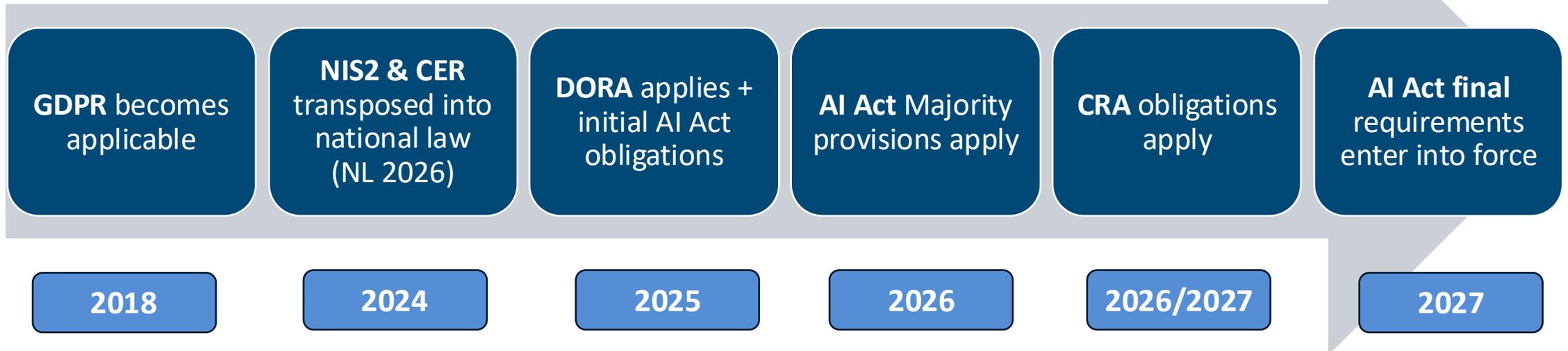
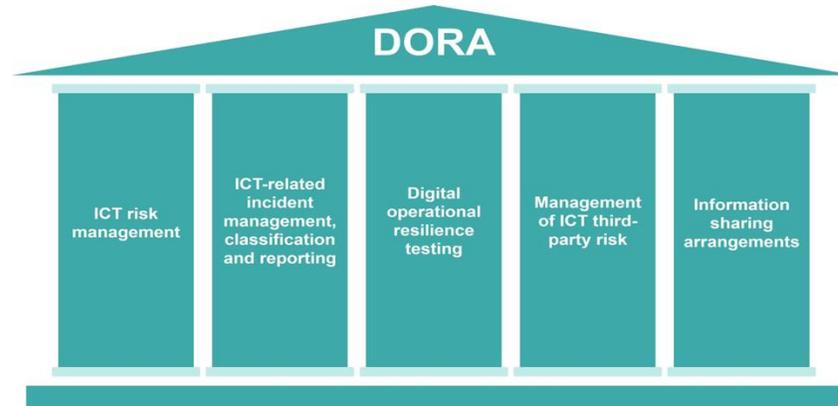
Many organizations position the CISO within IT under the CIO, limiting independence.



Regulation is supporting the CISO: Use it well!

CALL IN THE CISO
ACTUARIAL CONGRESS 2026 VSAE

Legislation



What do we see in practice?

Worst practices: “in letter”

Our supplier does have an assurance report (so we will be fine!).

We are compliant with DORA because we have a risk analysis (which has not been changed for the past five years).

Our supplier is testing for resilience (so we don't have to do anything ourselves).

Our technical systems do identify and archive technical incidents

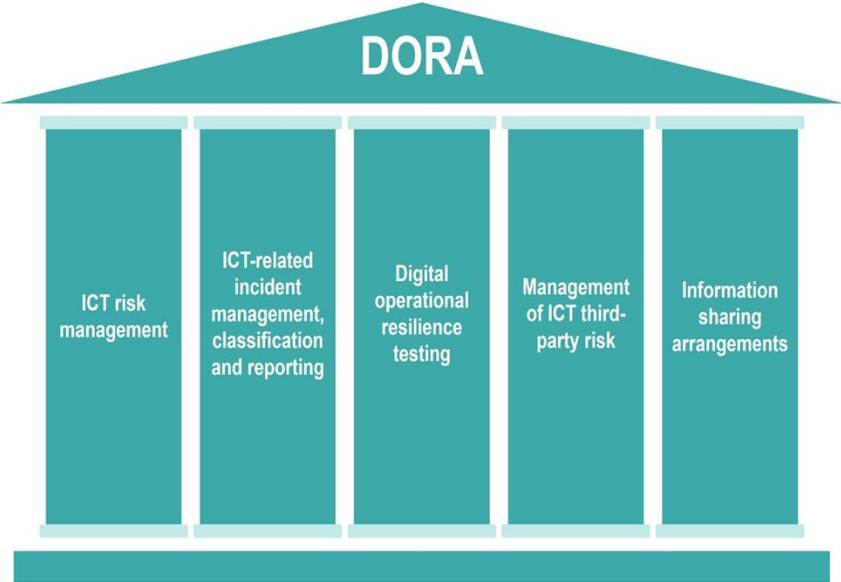
Best practices: “in spirit”

[Redacted]

[Redacted]

[Redacted]

[Redacted]





The CISO and the actuary

CALL IN THE CISO

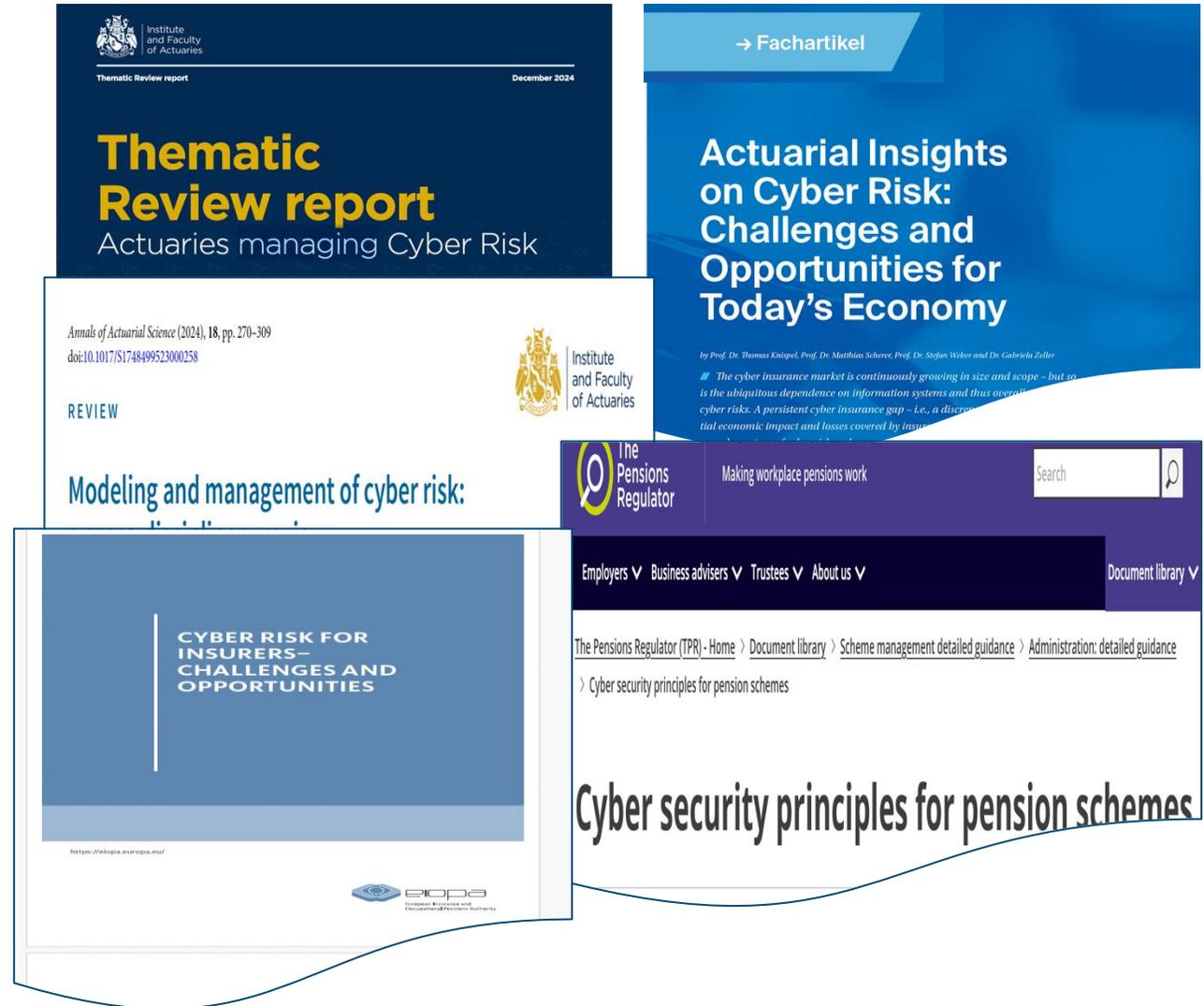
ACTUARIAL CONGRESS 2026 VSAE

3) What role does the actuary play in cyber risk management?

wooclap

CISO and the Actuary

- Operational risk measures
- Assessing financial impact cyber risks
- Products and Pricing
- Reserving and Capital
- Scenarios and Stress testing
- Risk mitigation (cyber insurance coverage)
- Data recovery





Wrap up

CALL IN THE CISO

ACTUARIAL CONGRESS 2026 VSAE

Wrap-Up: Importance of the CISO

01 The role of the CISO has become more important to guide the organizations in their cyber security strategy

Cyber incidents escalate beyond IT: triggering organization-wide operational, financial, and reputational crises.

Geopolitical tensions and AI increase cyber risks

02 The CISO is a strategic necessity, not a luxury

Without a CISO at the strategic table, organisations fly blind on digital risk, compliance gaps go undetected, and incidents escalate unchecked.

03 The CISO supports the organisation with

Effective implementation of regulation

Making sure the consequences in fat tails of cyber risk are better evaluated

Effective cyber insurance (pricing and coverage)

Thank you!



[HOME](#) | [ABOUT](#) | [SECTORS](#) | [SERVICES](#) | [INSIGHTS](#) | [CAREER](#) | [Q](#)

PROBABILITY
& PARTNERS

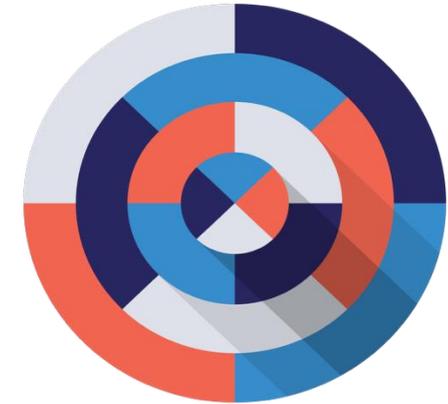


Banking

Insurance

Pensions

Asset Management



VSAA

The upcoming threats of
Artificial Intelligence

Papers and Bloggs on cyber risk topics (selection)

PROBABILITY & PARTNERS

HOME | ABOUT | SECTORS | SERVICES | INSIGHTS | CAREER | Q



Key risk management issues to consider when implementing DORA

By: Edward Roozenburg, Senior Risk management Consultant

On 17 January, all financial institutions must comply with the European regulation requiring financial institutions to be digitally resilient: the Digital Operational Resilience Act (DORA). Meanwhile, the financial institutions I work for have scheduled extra board meetings to adopt the latest changes to policy documents in time. This also provides work for the key risk management officer who provides the documents with a risk opinion. He also uses this moment to ask other questions about the implementation.

Edward Roozenburg
Senior Risk management Consultant

PROBABILITY & PARTNERS

HOME | ABOUT | SECTORS | SERVICES | INSIGHTS | CAREER | Q



DORA, are you ready yet?

With the approaching deadline for DORA of 17 January 2025, the pressure is mounting. For many financial institutions, being compliant on time is a challenge. What makes the implementation of these useful regulations complicated and what is best to focus on if you are running out of time?

On the face of it, DORA is a useful regulation that sets clear requirements for managing ICT risks of financial institutions. Straightforwardly drafted. At least that is what I myself thought when I first laid eyes on the text. It is a legal text in respect of a number of well-defined topics with some clear elaborations accompanied by templates. In fact, some of these templates are so clear that they can be copied exactly for an organisation. A matter of 'cut and paste'. But alas... reality turns out to be more complex than thought. So what actually makes it complex for pension funds and other financial institutions?

Edward Roozenburg
Senior Risk Management Consultant

PROBABILITY & PARTNERS

HOME | ABOUT | SECTORS | SERVICES | INSIGHTS | CAREER | Q



Exceptions to subcontractors registration in DORA?

Has your financial institution already determined which processes are important or critical?

By now, most of you will know that this must be determined to comply with the Digital Operational Resilience Act (DORA) that all European financial institutions must comply with from 17 January 2025. You probably also know that choosing which processes are critical or important is not optional. Because DORA specifies that for those suppliers providing services for critical or important processes, the subcontractors must also be identified.

In the Information Register, the financial institution must include all ICT suppliers including the subcontractors in case of outsourcing for critical or important processes. DNB has said it will request this register from all institutions in the second quarter 2025. AFM is already doing this at the end of the first quarter.

Edward Roozenburg
Senior Risk management Consultant

PROBABILITY & PARTNERS

AI and Machine Learning in Insurance: Can we ensure Fairness and Explainability?



By Svetlana Borovkova

PROBABILITY & PARTNERS

IT maturity and the DNB IT framework



Jeroen Kinders Vroklage, Renze Munnik & Pim Poppe

<https://probability.nl/publications/>

DORA is chefsache

Als je actief bent in de financiële sector, kan de komst van DORA (Digital Operational Resilience Act) je niet zijn ontgaan. Financiële instellingen hebben tot en met 17 januari 2025 om te voldoen aan deze EU-wetgeving, die erop gericht is de digitale weerbaarheid van financiële instellingen tegen cyberdreigingen te versterken.

Het is zeker niet nieuw dat je als organisatie moet beschermen tegen IT-risico's. Wel nieuw is dat deze regelgeving veel gedetailleerder en strikter is dan het huidige normenkader (onder andere de DNB Good Practice 2019/2020 en 2023), met meer directe regels en principes.

In de voorbereiding van een webinar over dit onderwerp heb ik een aantal organisaties gevraagd naar hun meest prangende vragen over DORA. Naast vragen over de verschillen met de huidige regelgeving en de vereisten voor IT-leveranciers (die ook aan DORA moeten voldoen) kwam de vraag langs waar in een organisatie de verantwoordelijkheid voor DORA-implementatie dient te liggen. Is dat nu de IT-afdeling, of risicomanagement, of misschien wel compliance? Een logische vraag. En ik zal heel eerlijk zijn, mijn reflex was om IT of risicomanagement te antwoorden. Maar het ligt toch iets anders.



Amba Zeggen
Sector Lead Insurance

Management aan zet

PROBABILITY & PARTNERS

AI Fairness in Financial Services

Trust at the Center

