



CYBER SECURITY
COALITION.be

EVERY LINK MATTERS

Cybersecurity in Belgium 2026

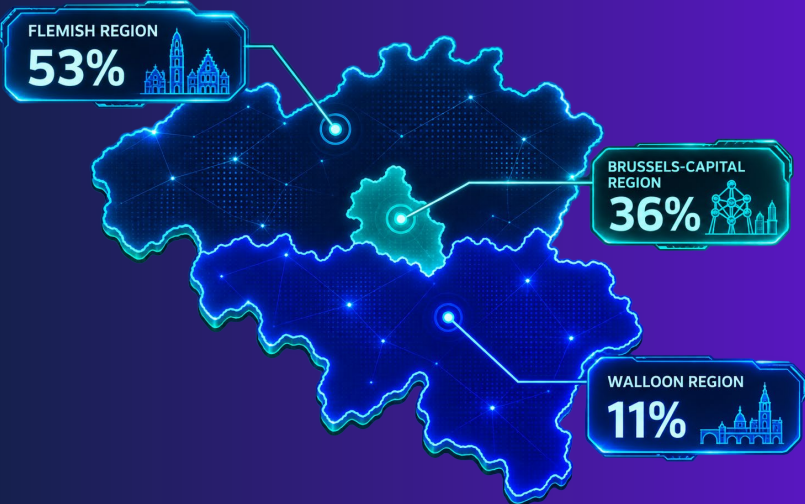
22/09/2026

La Sucrierie, Wavre



© 2026 KPMG Advisory, a Belgian BV/SRL and a member firm of the KPMG global organization of independent member firms affiliated with KPMG network, a private English company limited by guarantee. All rights reserved.

The Cybersecurity Study 2026



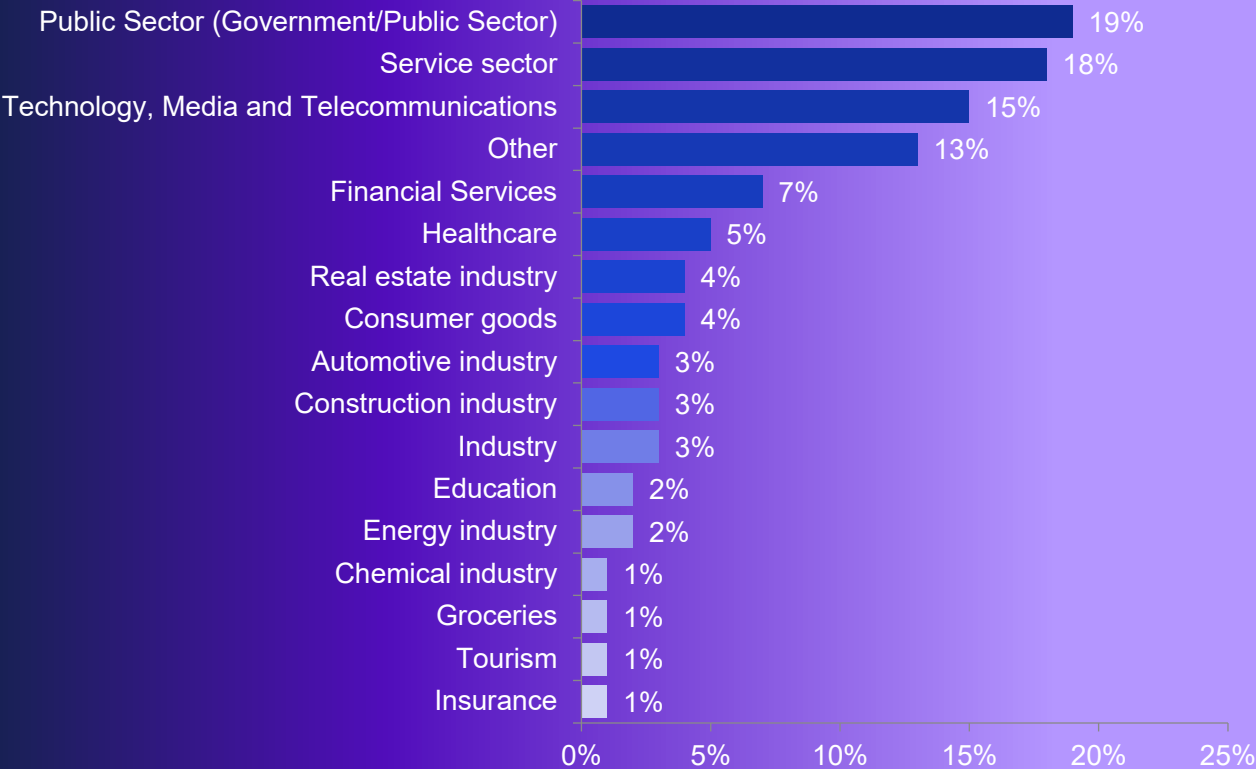
Participants

302



Questions

175



What the chain is made of

Resilience is not a single control. It is a chain and these are its links.



Leadership	People	Technology	Detection & response	Regulation	Third parties	Digital dependency	AI
Who owns the risk and who funds it	Everyone who touches a system	Identity, patching, the basics done well	How fast you notice and what you do next	Proving it works, not just having it	The suppliers inside your operations	The platforms it all runs on	New defence and new attack surface

A chain is only as strong as its weakest link. So where is this one weakest?

How strong is the chain?

The pressure has stopped being a surge. It is the baseline.

Under pressure



53%

report attacks increased



18%

were successfully attacked



44%

expect real damage

But moving forward



31→15%

of incidents go unreported



31→62%

report to CERT.be



29→16%

blind to supplier incidents

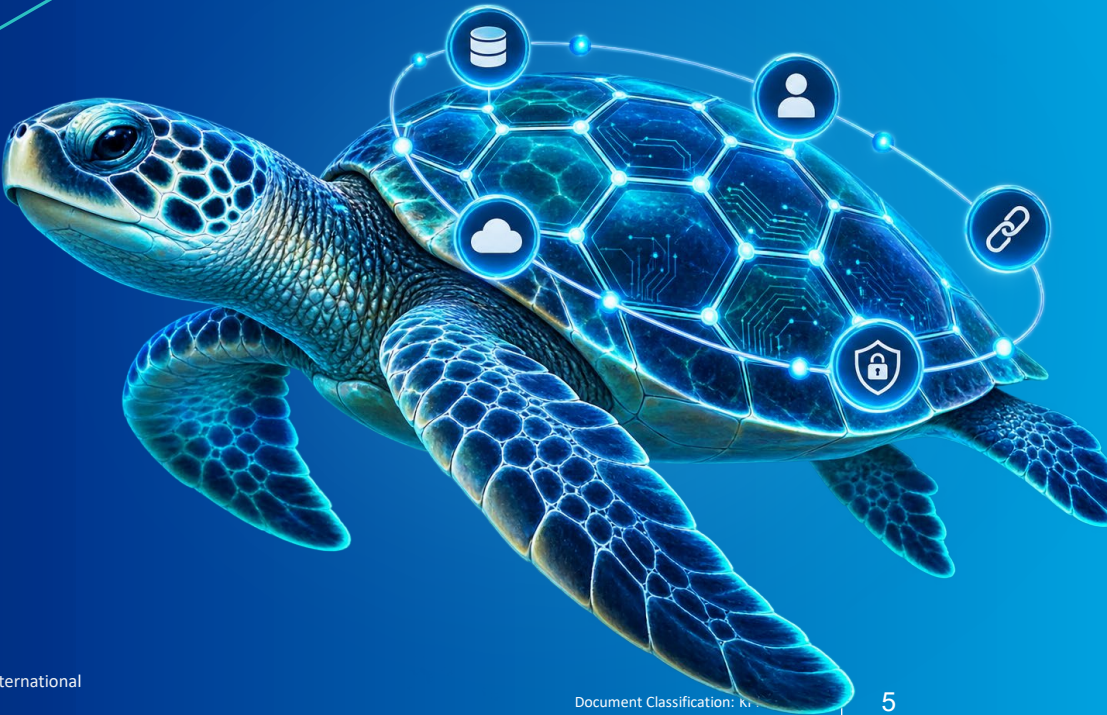
Where the strain moved

The loud attack is fading. The quiet one arrives through a trusted third party.



#11 → #3

Supply chain attacks — the largest single move in the ranking.



* Business Email Compromise

Five links under pressure

Maturity can no longer be judged control by control.



1

**Steering and
spending**

Perception outran
preparedness



2

**Regulation and
readiness**

Design outran
assurance



3

Us and our suppliers

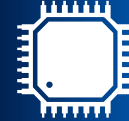
Concern outran
practice



4

**Dependence and
sovereignty**

Dependency we
cannot measure



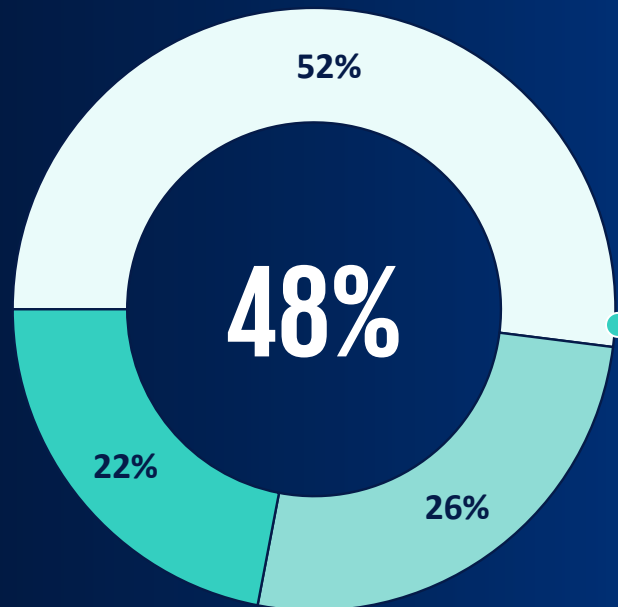
5

AI and integrity

Capability outran
governance

Steering and spending

Half the market cannot locate its cybersecurity budget.



- Has a designated budget
- Cannot say whether one exists
- No dedicated budget



36%

run cybersecurity with one or two people



42→65%

now use AI in cyber automation



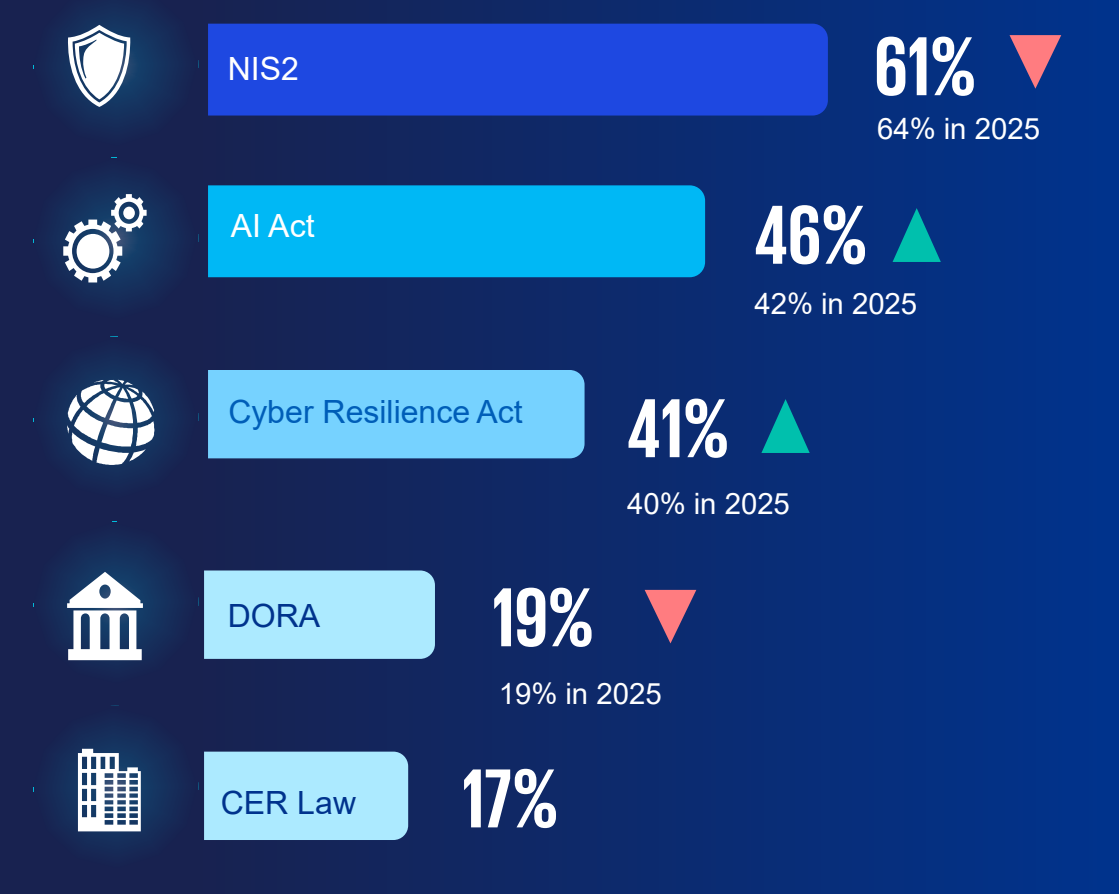
Perception has moved faster than preparedness.

Tabletop exercises fell from 52% to 40%.

Regulation and readiness

Which regulations are in scope?

Share of organizations affected



69%

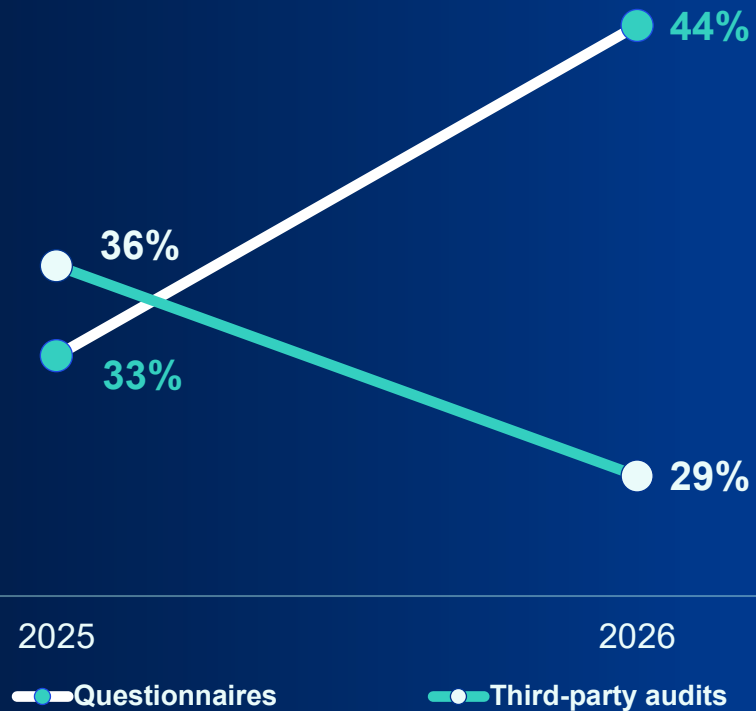
Say they are on track for the Belgian NIS2 deadlines



Us and our suppliers

Supplier assurance is getting broader and shallower at the same time.

How supplier assurance is verified



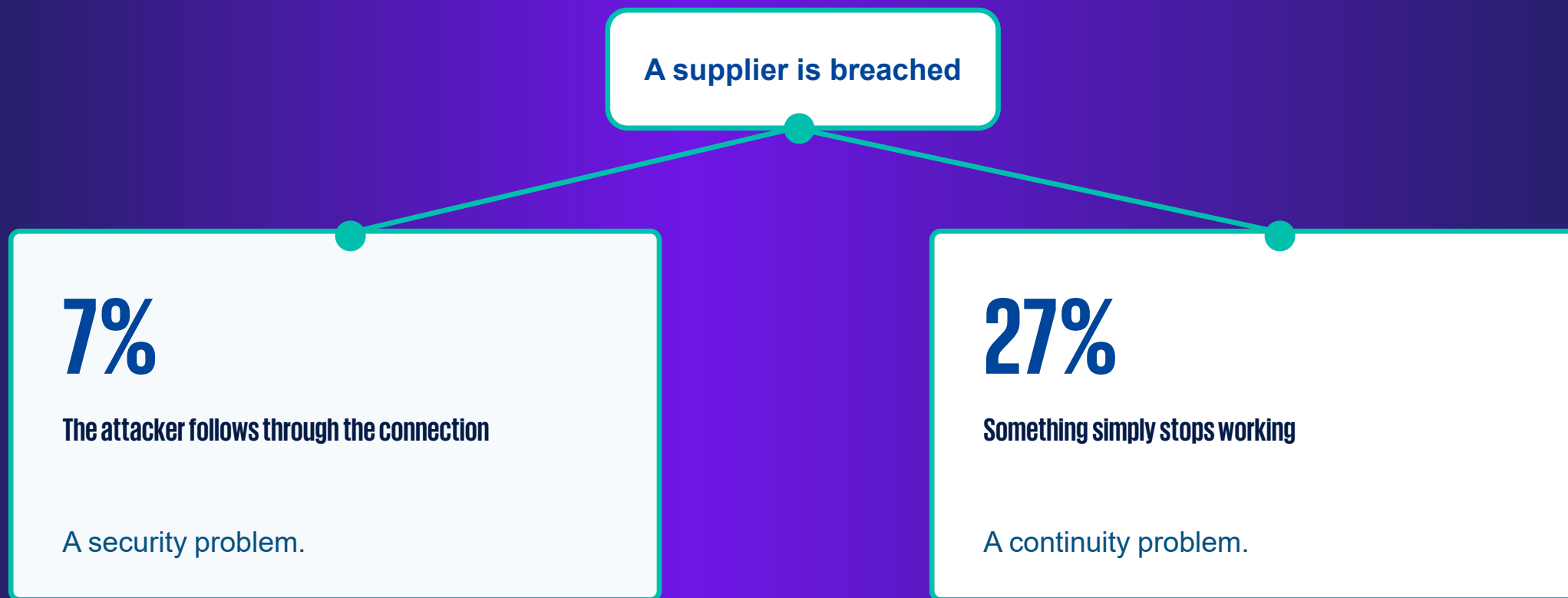
23%

do not know how their own organisation checks its suppliers

A self-declaration records that a question was asked. It does not establish that the answer was true.

What travels down the chain?

When a supplier is breached, the attacker usually doesn't arrive. The outage does.



Dependence & Sovereignty

The protective layer is the most import-dependent layer we have.

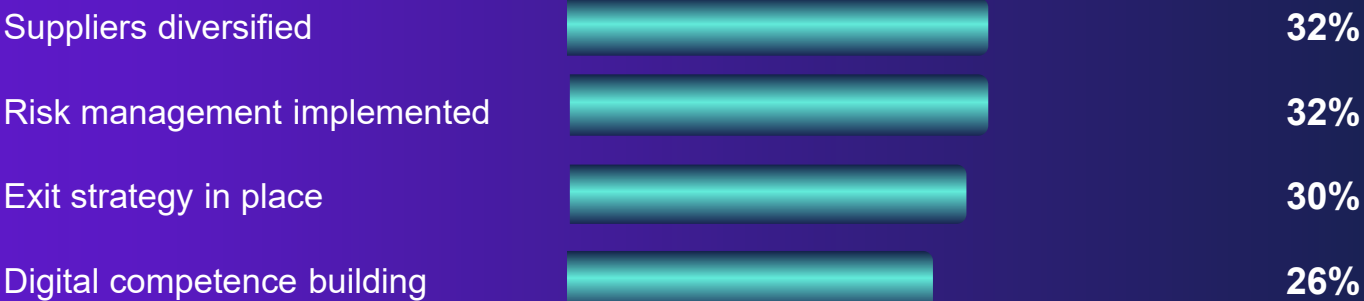
74%

Dependent from digital technology

41%

cannot say how long they would last
without foreign technology

Governance and process

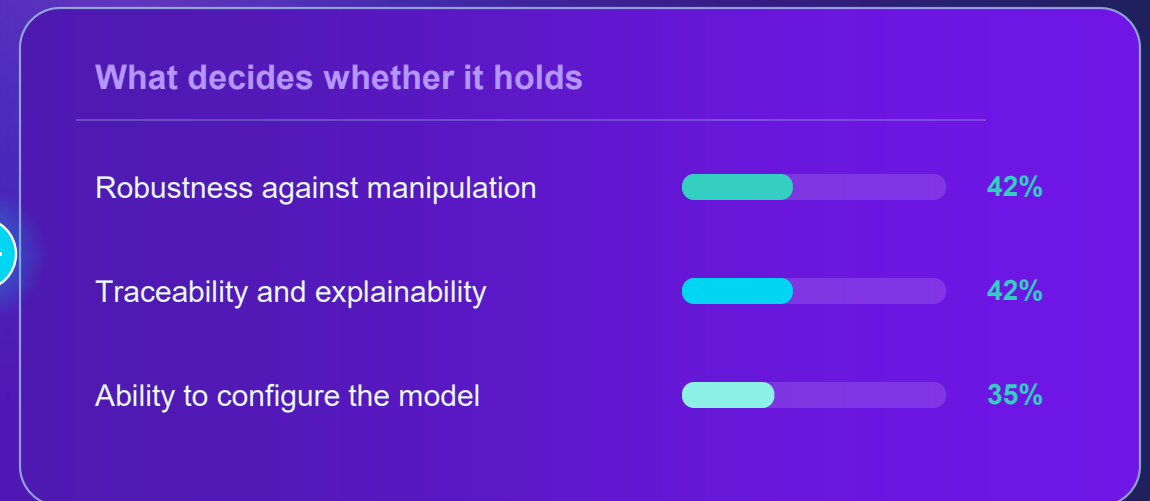
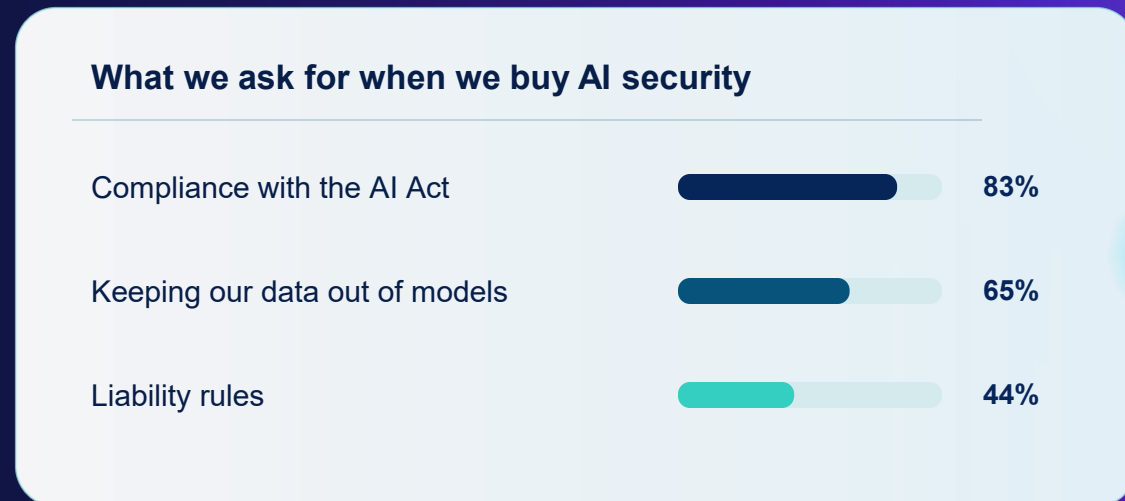


Architecture and technology



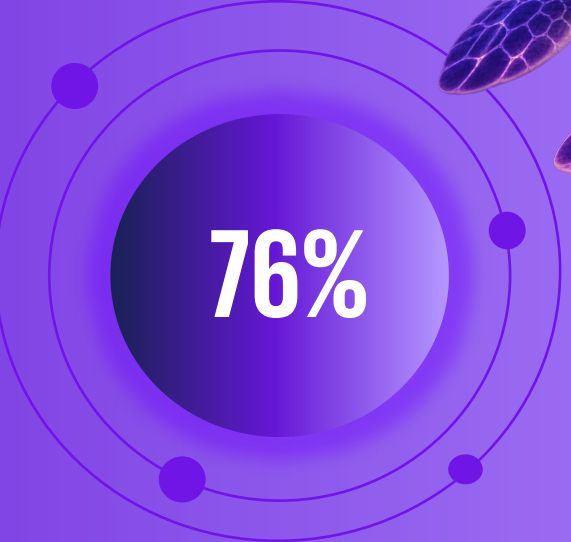
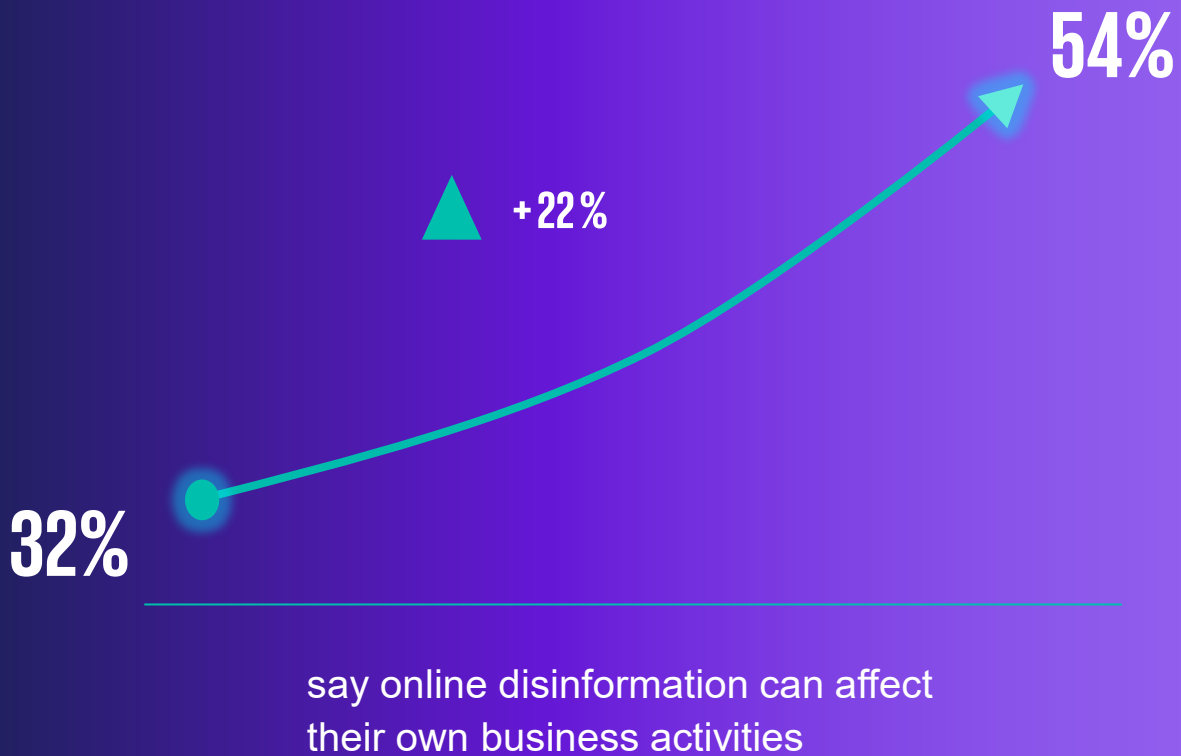
AI and integrity

Adopted faster than the rules for using it can be written.



Disinformation and trust

The largest single movement anywhere in the study.



Strengthening the chains

All of them exercises and measurements, not builds.



Test the 24-hour clock

1

Rehearse the notification path before April 2027.



Measure your runway

2

And your critical suppliers before you need it.



Make supplier assurance evidence-based

3

Audit rights and evidence, not questionnaires.



Govern AI at the speed you adopt it

4

Decision rights, provenance, human checkpoints.

Not on this list: new tooling

The links between organisations are becoming as important as the organisations themselves.

EVERY LINK MATTERS



The chain got stronger. The joints did not.



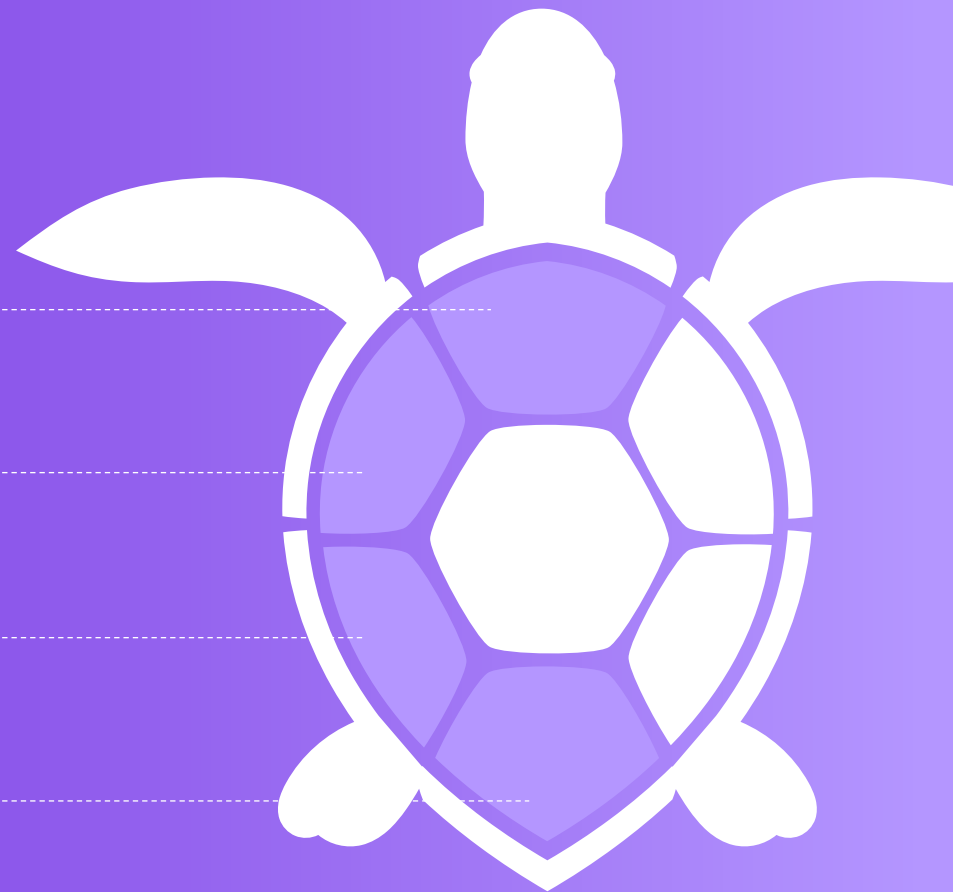
Visibility is becoming as important as protection.



The cheapest resilience available in 2027 is a rehearsal.



No organisation secures its own chain.



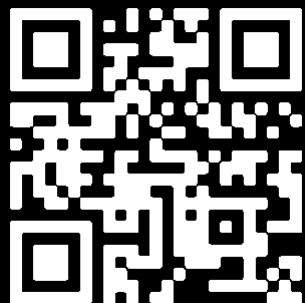


CYBER SECURITY
COALITION.be

Like the turtle, we may not always be the fastest — but with resilience, adaptability, and the right protection, we can endure any storm.

Where to download the full report?

1. KPMG in Belgium (<https://www.kpmg.be>)
2. Cyber Security Coalition (<https://cybersecuritycoalition.be/>)



Benny Bogaerts
Partner, Cyber Security Services



Benoit Watteyne
Partner, Cyber Security Services



Henk Dujardin
CEO, Cyber Security Coalition



Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.



kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

© 2026 KPMG Advisory, a Belgian BV/SRL and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Document Classification: KPMG Public