The IT landscape in motion

IT Channel Trend Report · Q4 2026

What is happening this quarter for IT partners and their SME customers: laws and regulations, sovereignty, threats, the market, and what you can do with it now.

IMMYTEC DATA PROTECTION & CYBERSECURITY

Contents

1	**This quarter at a glance**	Why this trend report · Five developments · Quarterly radar
2	**Laws and regulations**	Cybersecurity Act (NIS2) · European regulation · Supply chain
3	**Sovereignty and cloud**	Policy and government · Market and offering
4	**Threats and resilience**	Threat landscape · Incidents · SME resilience · Cyber insurance
5	**The market for IT service providers**	Market in figures · Vendors and prices · Labour market · Customer · Strategic questions
6	**In depth**	Sector in the spotlight · Technology on the radar
7	**Getting started**	Schemes · Agenda · Deadlines · Conversation starters

Why this trend report

There is no shortage of information on legislation, threats and the market. The problem is that it is fragmented.

Any IT partner who wants to keep up has to look in dozens of places: government and regulators, European regulation, trade media, research reports and vendors. Each has its own pace and perspective, so it becomes hard to know where to find what. We see a growing need for one place where it all comes together.

Every quarter, this trend report brings together what is going on, organises it into fixed sections and cites the source for every fact. That way you can see at a glance what has changed, what is coming and how you can use it in conversations with customers.

- Government and regulators
- European regulation
- Threat assessments
- Research reports
- Trade media
- Vendors and distributors
- Industry associations
- Events and trade fairs

→

One overview

bundled, organised, sourced, every quarter

Five developments since July 2026

01 Cybersecurity Act in force

Since 15 August 2026, registration, duty-of-care and reporting obligations apply to more than 8,000 organisations. SMEs feel the effects through the supply chain.

02 Government opts for maximum sovereignty

Central government tightened its cloud policy and is building its own government cloud. The takeover of DigiD operator Solvinity did not go ahead.

03 Threats grow faster than resilience

Cyber Security Assessment Netherlands 2026: AI is accelerating attacks, and vulnerabilities are exploited within hours.

04 Cyberattack hits the retail chain

Ahold Delhaize expects €200–250 million less revenue in the fourth quarter as a result of the October incident.

05 Licences and hardware more expensive

Microsoft raised several 365 prices from 1 July; memory prices rose sharply due to demand from AI.

8,000+
organisations fall under the Cybersecurity Act (NCSC)

84%
of Dutch IT decision-makers consider data sovereignty important or a top priority (Leaseweb)

136
ransomware attacks recorded by the Dutch Data Protection Authority in 2025

What is new, what is ongoing and what is coming

The radar places developments on a timeline: what took effect this quarter, what is still ongoing and what to keep in mind over the coming months.

New	Cybersecurity Act in force (15 August) · Cyber Resilience Act reporting obligation started (11 September) · Cyber Security Assessment Netherlands 2026 published (6 November)
Ongoing	Registration of organisations with the NCSC · Transition to the stricter central government cloud policy · Rising prices for memory and hardware
Coming up	Grant scheme for small businesses closes 30 November · First applications on the government cloud by end of 2026 · Cyber Resilience Act fully applicable on 11 December 2027

02

Laws and regulations

Which rules apply now, what they require and how they ripple through the supply chain, including to organisations that are not covered themselves.

2.1 Cybersecurity Act (NIS2)
2.2 European regulation: CRA and AI
2.3 Impact on the supply chain

IMMTEC DATA PROTECTION & CYBERSECURITY

The Cybersecurity Act is in force

Since 15 August 2026, the Cybersecurity Act (Cyberbeveiligingswet, Cbw), the Dutch implementation of the European NIS2 Directive, and the Critical Entities Resilience Act (Wwke) have applied. The act imposes four obligations.

- **Registration:** in the NCSC entity register. Organisations determine for themselves whether they fall under the act.
- **Duty of care:** appropriate and proportionate measures based on a risk analysis.
- **Reporting obligation:** early warning within 24 hours, notification within 72 hours and a final report within one month.
- **Management:** approves the measures, oversees them and completes training.
- **Who is covered?** Organisations in a designated sector with 50 or more employees, or with turnover or a balance sheet total above €10 million.

8,000+
organisations under the Cbw

±500
organisations under the Wwke

18
sectors

24 hours
for the early warning

Source: Rijksoverheid (15-08-2026); NCSC, Cyberbeveiligingswet: meldplicht and 'Valt mijn organisatie onder de Cbw?'

Cyber Resilience Act and AI: the next wave

Alongside NIS2, which is about organisations, European regulation is coming for products and for AI. Both affect IT partners: as suppliers of hardware and software, and as advisers on the introduction of AI.

CYBER RESILIENCE ACT (CRA)

- Since 11 September 2026, manufacturers must report actively exploited vulnerabilities and severe incidents: within 24 hours, within 72 hours and with a final report.
- From 11 December 2027, most obligations apply. Fines of up to €15 million or 2.5% of worldwide turnover.
- Anyone who sells products under their own name or substantially modifies them may take on the obligations of a manufacturer. That can include a reseller.

AI: USAGE IS AHEAD OF POLICY

Since 27 July 2026, the AI omnibus has amended the European AI Act. For SMEs, AI is already everyday practice, but agreements are often missing:

8 in 10
SMEs use AI to some extent

1 in 3
fear sensitive data ends up in AI tools

9%
of SMEs have a formal AI policy

Source: Jones Day (07-2026); Integrity360 (31-08-2026); European Commission, AI Office; AI figures from the Cybersecuritybeeld 2026 as reported by ICT Magazine (10-11-2026)

Even those not covered by the act will feel it

Most SMEs do not fall under the Cybersecurity Act. But organisations that do must manage their risks, and that includes their suppliers. That is how the questions end up with SMEs, and with their IT partner.

Cyber Security Assessment Netherlands 2026 puts it this way: small organisations and SMEs cannot raise their resilience on their own. Suppliers, regulators and government share responsibility.

QUESTIONS SME CUSTOMERS WILL BE ASKED MORE OFTEN

1. Do you have an up-to-date overview of your systems and who has access to them?
2. How quickly, and through which channel, will you report an incident to us?
3. Are your backups tested, and out of an attacker's reach?
4. Which jurisdiction is your cloud provider subject to?
5. Has your continuity plan actually been rehearsed?

Source: NCSC (06-11-2026) on the Cybersecuritybeeld 2026; questions derived from the duty of care in the Cybersecurity Act

03

Sovereignty and cloud

Why the government is opting for maximum control over data and infrastructure, and how the topic is reaching SMEs.

3.1 Policy and government
3.2 Market and offering

IMMUTEC DATA PROTECTION & CYBERSECURITY

The government chooses the highest level of sovereignty

On 3 July 2026, the cabinet tightened the central government's cloud policy. Formally it applies only to central government, but it sets the tone for what large clients will ask of their suppliers.

- A cloud strategy drawn up in advance that covers the risks, such as dependence on a single supplier and non-European law
- A mandatory exit plan for important cloud services
- Email and documents: public cloud discouraged
- Critical organisations: providers subject to non-EU law discouraged for core tasks
- A dedicated government cloud at the highest level (SEAL-4) of the EU Cloud Sovereignty Framework; first applications by end of 2026
- Four years to adapt existing services

CASE: SOLVINITY AND DIGID

Nov 2025	US-based Kyndryl wants to acquire Solvinity, the company behind the DigiD infrastructure
26 May 2026	The State Secretary blocks the takeover on the advice of the Investment Screening Office (BTI)
Aug 2026	Kyndryl abandons the takeover
2028	The cabinet then wants a Dutch or European party for DigiD

Source: Rijksoverheid (03-07-2026); Computable (03-07-2026); NOS (26-05-2026); MSP Business (27-08-2026)

From government file to SME conversation

Sovereignty is no longer just a topic for government. Research among Dutch organisations shows that it is starting to steer IT strategy. Customers are not switching en masse, but they do want to know where they stand.

84%

of 383 Dutch IT decision-makers call data sovereignty important (61%) or a top priority (23%). *Leaseweb, 2026*

37%

of large organisations say sovereignty influences their IT strategy. *Dutch IT Sourcing Study 2026*

26%

want to become less dependent on the large cloud providers; 45% in the public sector. *Dutch IT Sourcing Study 2026*

SOVEREIGNTY OR AUTONOMY?

Sovereignty is about jurisdiction: which law applies to your data? Autonomy is about freedom of choice: do you know where your data is, and can you leave if you have to?

WHAT AN IT PARTNER CAN DO WITH THIS

Start with insight: where is which data, what dependencies exist, and what is the exit scenario for each critical service? That conversation is also possible within a Microsoft environment.

Source: Leaseweb/Blauw via Accountant.nl (10-06-2026); Eraneos and Whitelane, Dutch IT Sourcing Study 2026; Computable (21-04-2026)

04

Threats and resilience

How is the threat developing, which incidents stood out, and how resilient are SMEs really?

4.1 Threat landscape
4.2 Incidents and figures
4.3 SME resilience
4.4 Cyber insurance

IMMUTEC DATA PROTECTION & CYBERSECURITY

Threats are growing faster than resilience

On 6 November 2026, the NCTV and NCSC published Cyber Security Assessment Netherlands 2026. Its core message is a growing imbalance: attackers are becoming more capable, while organisations' digital resilience is lagging behind.

AI in every phase

Attackers use AI in every phase of an attack. Widely available models are enough for malware and convincing phishing.

From months to hours

The time between discovery and exploitation of a vulnerability: months in 2024, weeks in 2025, only a few hours in 2026.

Extortion through data theft

Criminals are increasingly focused on stealing data. There were more incidents with major societal impact.

Assume a breach

Keeping intruders out is not enough. What matters is detecting and stopping them quickly.

NCSC and NCTV advice: executive ownership · patch quickly · backups and tested continuity · 24/7 logging and detection · insight into your own IT landscape

Source: NCTV and NCSC, Cybersecuritybeeld Nederland 2026 (06-11-2026); Computable (06-11-2026)

Ransomware in figures and the case of the quarter

Each year, the Dutch Data Protection Authority (AP) counts the ransomware attacks that led to a data breach. In addition, every quarter we highlight one incident that shows what an attack means in practice.

DUTCH DATA PROTECTION AUTHORITY ON 2025

136
ransomware attacks (2024: 127)

283
data breaches reported as a result: one attack often affects several organisations

Attacks involving only data theft, without encryption, rose from 15 to 32. The AP's advice: don't pay, and make sure you have recent backups that were not affected by the attack.

CASE: AHOLD DELHAIZE, OCTOBER 2026

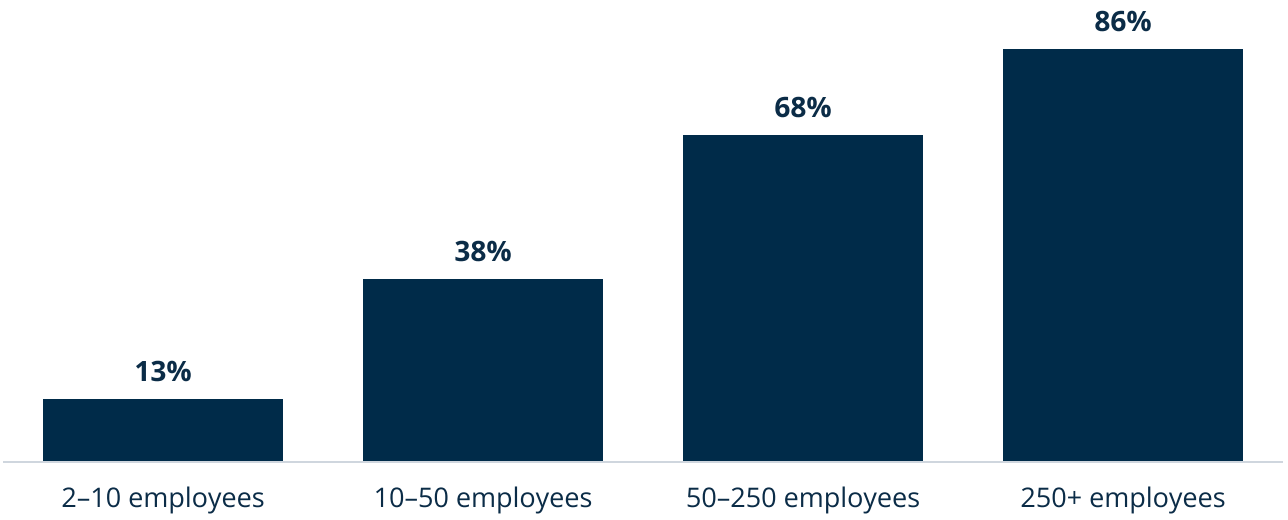
- On 12 October, the group reported a cyber incident; systems were taken offline as a precaution
- Websites, apps and home delivery of Albert Heijn, among others, were down; delivery for around two weeks
- Expected impact in Q4: €200–250 million in revenue
- According to the company, no indication that customer or partner data was stolen

Source: AP, Rapportage ransomware 2025 (07-2026) via ICT Magazine and AG Connect; Ahold Delhaize (13-10-2026); ICT Magazine (04-11-2026)

The smaller the company, the fewer the measures

Each year, Statistics Netherlands (CBS) measures which of twelve security measures companies take, such as backups, encryption and two-factor authentication. The chart shows, by company size, the share that has ten or more of those measures.

Share of companies with ten or more of the twelve security measures



WHAT THIS SHOWS

Of the smallest companies, 13% have the basics broadly in place, compared with 86% of large ones. The very group that most SME customers belong to is the most vulnerable.

33%
of companies with 2–10 employees encrypt data

91%
of companies with 250+ employees do so

Source: CBS, Cybersecuritymonitor 2025 (28-05-2026)

Insurers increasingly set the baseline

Insurers set requirements before covering a cyber risk, and when a claim is made they check whether the measures were actually in place. For IT partners, those requirements are therefore becoming a recognisable baseline in conversations with customers.

19%

of Dutch companies are insured against cyber incidents; 35% in the ICT sector (CBS)

−4%

drop in cyber premiums worldwide in Q2 2026, the twelfth consecutive quarter (Marsh)

Premiums are falling, but the requirements are not getting any looser. That makes this a good moment to discuss with customers whether they are insured, and whether they meet the conditions.

WHAT INSURERS USUALLY ASK FOR

- Multi-factor authentication (MFA) on email, remote access and admin accounts
- Endpoint detection (EDR), with 24/7 monitoring for larger policies
- Offline or immutable backups with tested recovery
- Fixed timeframes for updates
- An incident response plan and awareness training

Note: an incorrectly completed questionnaire can cost you your cover.

Source: CBS, Cybersecuritymonitor 2025 (28-05-2026); Marsh Global Insurance Market Index Q2 2026 (23-07-2026); requirements according to MSP Business (01-10-2026) and Q-Cyber (commercial)

05

The market for IT service providers

How is the market for MSPs and IT resellers changing: consolidation, vendors, people and what customers expect.

5.1 Market in figures
5.2 Vendors, prices and licences
5.3 Labour market and capacity
5.4 The customer in focus
5.5 Strategic questions for IT partners

IMMTEC DATA PROTECTION & CYBERSECURITY

Consolidation continues

The Dutch managed services market is consolidating rapidly. Investors are building platforms by merging MSPs. The figures come from M&A adviser Hogenhouck m&a, which itself advises on MSP acquisitions.

219
acquisitions in the Dutch MSP segment from 2023 to 2025

88%
of those acquisitions involved an investor

±6
transactions per month in 2025 and 2026

$1M
in annual CSP revenue that Microsoft now requires from direct-bill partners

WHAT BUYERS LOOK FOR

- Recurring revenue and long contracts
- A spread across customers
- Specialisation in security, cloud or a sector

AI: FEAR AND ACCELERATOR

At MSP Global (October 2026, more than 2,000 visitors), AI was the main theme. MSPs are busy with it, but rollout to customers is lagging behind.

Source: Hogenhouck m&a via TBM (12-02-2026) and Consultancy.nl (05-05-2026); Microsoft Partner Center; c't (27-10-2026)

Licences and hardware are getting more expensive

Two cost items rose at the same time this year: Microsoft licences and hardware. For IT partners that means difficult conversations about prices, but also a reason to review licences and replacement with customers.

MICROSOFT 365 FROM 1 JULY 2026 (LIST PRICE IN USD)

Licence	Old	New
Business Basic	$6.00	**$7.00**
Business Standard	$12.50	**$14.00**
Business Premium	$22.00	**$22.00**
Office 365 E3	$23.00	**$26.00**
Microsoft 365 E3	$36.00	**$39.00**
Frontline F3	$8.00	**$10.00**

Per user per month, versions with Teams. The new price applies at renewal; prices in euros may differ.

HARDWARE: AI IS CLAIMING THE MEMORY

+90–95%

expected rise in DRAM contract prices in the first quarter of 2026 (TrendForce)

Manufacturers supply AI data centres first. As a result, PCs, laptops and servers have become more expensive. Advice: lock in replacement planning and quotes early.

Source: Microsoft, 2026 M365 Packaging and Pricing Updates (16-02-2026); TrendForce (02-02-2026)

The shortage is easing, but not for specialists

For years, staff shortages were the biggest brake on growth in IT. That picture is shifting: the number of vacancies is falling and employers experience fewer shortages. Specialist roles remain hard to fill.

589,000
people work in an ICT occupation; the number has been rising since 2023

18,900
open ICT vacancies in the second quarter of 2026; falling since 2023

29%
of employers in information and communication cite staff shortages as an obstacle (2022: 53%)

WHAT IS CHANGING

- The number of unemployment benefit claims from ICT is rising, partly due to reorganisations
- AI automates tasks and demands more specialist knowledge

WHAT AN IT PARTNER CAN DO WITH THIS

Less scarcity creates room for targeted recruitment and training your own people in security and AI: the expertise customers are asking for.

Source: UWV, Arbeidsmarktinformatie ICT-beroepen (10-2026) and Werkgeversonderzoek 2025 (02-2026)

What customers expect from IT service providers

The Dutch IT Sourcing Study 2026 by Eraneos and Whitelane surveyed more than 350 large Dutch organisations about their IT suppliers. These are large organisations, but the criticism will also sound familiar to SME service providers.

WHERE CUSTOMERS SAY SUPPLIERS FALL SHORT

45% do not challenge the customer enough

30% do not understand the customer's business well enough

25% do not behave like a true partner

ALSO NOTABLE

- Average satisfaction with suppliers: 75%
- 26% want to do more themselves; five years ago this was 12 to 13%
- 15% already see significant impact of AI on their business; a year earlier 2%
- Main reason to outsource: scalability (53%)

Source: Eraneos and Whitelane Research, Dutch IT Sourcing Study 2026 (03-2026); Computable (21-04-2026)

Six strategic questions

No answers, but lines of thinking. Each question follows from the developments in this report.

Scale or specialisation?

Consolidation rewards scale, but customers and buyers look for specialists. Where does your differentiation lie?

Compliance as a service?

The Cbw, the CRA and ISO 27001 demand demonstrable compliance. Can that become a standing service rather than a project?

How sovereign is the portfolio?

Do you know, for each service, where customer data is stored, which law applies and what the exit scenario is?

Who oversees AI use?

Most SMEs use AI, few have a policy. Who helps with agreements, access rights and awareness?

How do you prove continuity?

Demonstrably and periodically testing recovery is a conversation for the board, not just for IT.

Which partners complement you?

No one has to build everything themselves. Spreading responsibility also reduces the risk for the customer.

06

In depth

Each quarter, one sector in the spotlight and the technologies that will affect IT partners in the coming years.

6.1 Sector in the spotlight: retail, wholesale and automotive
6.2 Technology on the radar

IMMTEC DATA PROTECTION & CYBERSECURITY

Retail, wholesale and automotive

According to the AP, retail and the automotive sector are among the three sectors with the most data breaches caused by ransomware. Companies in this sector run on systems that must always be available, and sit in the middle of a supply chain.

Top 3
retail and automotive in ransomware data breaches in 2025, after healthcare and ahead of ICT (AP)

6 in 10
wholesale and retail companies did not know their own NIS2 obligations in 2025 (ABN AMRO)

WHY VULNERABLE

- ERP, warehouse and webshop must run continuously
- Many integrations with suppliers and carriers
- Downtime has an immediate knock-on effect: from distribution centre to shelf

RECENT EXAMPLES

- Ahold Delhaize (October 2026): online and distribution partly down
- Ceva Logistics (August 2026): customer data of at least twelve clients leaked
- Blue Yonder (November 2024): supply chain software down, supermarkets affected

Source: AP, Rapportage ransomware 2025 via AG Connect (30-07-2026); ABN AMRO (14-07-2025); ICT Magazine (04-11 and 10-11-2026)

What the sector needs from IT partners

IS THE CUSTOMER COVERED BY THE CYBERSECURITY ACT?

Food is one of the designated sectors. A company in such a sector falls under the act if it has 50 or more employees, or turnover or a balance sheet total above €10 million. In doubt? The NCSC self-assessment provides clarity. Trading companies that are not covered will still get questions from customers that are.

What does a day of downtime cost?

Revenue per day + wage costs of employees who cannot work + recovery + contractual damages. A concrete figure makes continuity a topic the board will discuss.

CONVERSATION TOPICS FOR THIS SECTOR

1. How long can the warehouse keep running without ERP?
2. Are all integrations with suppliers and the webshop mapped?
3. Has recovery of the ERP system ever been tested?
4. Who reports an incident to customers in the supply chain, and how quickly?
5. Do the measures meet the insurer's requirements?

Source: NCSC, 'Valt mijn organisatie onder de Cyberbeveiligingswet?'

Four developments to watch

Not every technological development calls for action now. The radar divides them into what matters now, what is coming soon and what will become relevant later, so you know where to build up knowledge.

NOW

AI assistants

15% of large organisations already see significant impact of AI, compared with 2% a year earlier. Policy, access rights and data labelling become basic work in every rollout.

NOW

24/7 detection and response

The NCSC and NCTV advise continuous logging, monitoring and detection. Insurers also require it for larger policies.

SOON

Farewell to Windows 10

Support ended in October 2025. Extended security updates cost $61 per device in the first year and double each year, for a maximum of three years.

LATER

Quantum-safe encryption

According to the European roadmap, high-risk applications must have migrated by the end of 2030. The NCSC advises taking inventory now.

Source: Eraneos and Whitelane (03-2026); NCTV (06-11-2026); Microsoft Learn, Extended Security Updates; NCSC, Quantumveilige cryptografie

07

Getting started

Schemes, events, deadlines and questions to open the conversation with customers.

7.1 Schemes and resources
7.2 Agenda
7.3 Deadlines and milestones
7.4 Conversation starters

IMMUTEC DATA PROTECTION & CYBERSECURITY

What is available for SMEs now

For small businesses there is a grant and free help to get the basics in order. A concrete reason to talk to small customers before the end of the year.

APPLICATIONS UNTIL 30 NOVEMBER 2026

Mijn Cyberweerbare Zaak grant

50%	€1,250	€1M
of the cost of measures	maximum per applicant	available in 2026

For small businesses and freelancers. Complete the CyberVeilig Check, purchase the measures, keep the invoices and apply through the Netherlands Enterprise Agency (RVO).

ALSO AVAILABLE

- CyberVeilig Check: the starting point for the grant
- NCSC: basic principles for digital resilience
- NCSC self-assessment: does my organisation fall under the Cbw?
- The cabinet's Future-Proof Digital Resilience Action Programme, including better preparation of SMEs

Source: NCSC, ncsc.nl/subsidie; NCTV (06-11-2026)

Agenda: MSPs, cloud and security

Date	Event	Location	What it is
2–3 Dec 2026	Cloud Expo	Expo Houten	Trade fair on cloud, AI and data
11 Dec 2026	Making CRA a Reality	ENISA / European Commission	Explanation of the Cyber Resilience Act
19 Jan 2027	Yellowhat	Almere	Microsoft Security event for SOC analysts and MSSPs
1–3 Mar 2027*	IT Nation Connect Europe	London	ConnectWise event for MSPs
15–18 Mar 2027	CloudFest	Rust (Germany)	International event for cloud and hosting
17 Mar 2027	NLdigital Ondernemersdag	Woerden	Annual day of the industry association for IT companies
26–27 May 2027	Cybersec Europe	Brussels	Security fair including OT and AI security
31 May–1 Jun 2027	Experts Live Netherlands	Nieuwegein	Microsoft community event for IT professionals
8–10 Jun 2027	Infosecurity Europe	London	Major European security fair
22–24 Jun 2027	Kaseya Connect Europe	TBA	Kaseya event for MSPs
14 Sep 2027	MSP Show NL and SITS	Jaarbeurs Utrecht	Trade fair and seminars for MSPs, free admission
15–16 Sep 2027	Cybersec Netherlands	Jaarbeurs Utrecht	Security fair for experts and start-ups
5–6 Oct 2027	ONE Conference	TBA	Cybersecurity conference by the NCSC, among others
5–7 Oct 2027	it-sa Expo&Congress	Nuremberg	European trade fair for IT security

* Date from a third-party overview; the organiser's website could not be checked.

Source: organisers' websites and it-agenda.nl, checked on 12-11-2026; IT Nation: nuoptima.com (08-2026)

Agenda: other disciplines and sectors

Date	Event	Location	What it is
19–23 Jan 2027	NOT	Jaarbeurs Utrecht	Education: trade fair for education and childcare
28 Jan 2027	Nationale Privacy Conferentie	The Hague	Privacy: ECP conference
2–5 Feb 2027	Integrated Systems Europe (ISE)	Barcelona	AV and systems integration
16–17 Feb 2027	Kickstart Europe	Amsterdam	Data centres and cloud infrastructure
16 Mar 2027	Security Leadership	Utrecht	For CISOs and IT management
13–15 Apr 2027	Zorg & ict	Jaarbeurs Utrecht	Healthcare: largest health tech fair in the Netherlands
13 Apr 2027	IT Asset Management	Vianen	Licence and asset management
21 Apr 2027	Cloud & AI in de Publieke Sector	Utrecht	Government: digitalisation and infrastructure
20 May 2027	Identity & Access Management	Den Bosch	Access management, for IAM managers and CISOs
2 Jun 2027	Cyberweerbare Overheid	The Hague	Government: for CISOs and ICT managers
15–16 Sep 2027	Data Expo	Jaarbeurs Utrecht	Data, AI and business intelligence
9 Nov 2027	AI & Automation Day	Utrecht	AI and automation in business operations
25 Nov 2027	Cyber Security Experience	Utrecht	For security and ICT managers

Events outside your own bubble: this is where you meet customers' IT leads in healthcare, education, government and industry.

Source: Jaarbeurs, zorg-en-ict.nl, data-expo.nl, iseurope.org, heliview.com and it-agenda.nl, checked on 12-11-2026

Dates to keep an eye on

The key dates from this report at a glance, in chronological order.

30 Nov 2026	**Last day for the Mijn Cyberweerbare Zaak grant**
End of 2026	First applications on the sovereign government cloud
End of 2026	National quantum roadmap per EU member state
11 Dec 2027	Cyber Resilience Act fully applicable
2028	The cabinet wants a Dutch or European party for DigiD
2030	End of the four-year transition period for the central government cloud policy
End of 2030	High-risk applications quantum-safe (EU roadmap)

Source: NCSC; Rijksoverheid (03-07-2026); Computable (03-07-2026); Jones Day (07-2026); MSP Business (27-08-2026)

Ten questions to discuss with customers

Every development in this report can be translated into a simple question for a customer. Not a sales pitch, but an opening for a good conversation.

01	Do you supply organisations that fall under the Cybersecurity Act?
02	What does one day of downtime cost, in euros?
03	When was recovery of your systems last tested?
04	Can an attacker who is already inside reach your backups?
05	Which jurisdiction are your main cloud services subject to?
06	Do you have an exit scenario for your critical services?
07	Which AI tools do your employees use, and with what data?
08	Who on the board owns cyber risk?
09	Do you meet the requirements of your cyber insurance?
10	Has your incident response plan ever been rehearsed?

About this trend report

The IT Channel Trend Report is published every quarter and brings together what is going on for IT partners and their SME customers. The content is based on public sources and reflects the situation at the time of publication. This report is not legal advice.

IMMUTEC is a European Managed Service Provider for data protection and cybersecurity. You may share and reuse this report, with attribution. Sources are cited on each page; ‘via’ means that a figure was taken from an intermediary source.

NEXT EDITION

Q1 2027

immutec.eu · info@immutec.eu · +31 (0)85 482 3400

IT Channel Trend Report Q4 2026 · EN V0.1 · Errors and omissions excepted.

IMMUTEC DATA PROTECTION & CYBERSECURITY