Five AI developments of 2026 that impact how boards work

Introduction to the Swiss Board Forum AI Circle for Members of Boards of Directors

1 VALUE

2 AGENTS

3 CYBER

4 COMPUTE

5 BOARDS

Martin Söderberg, AI assisted research, October 19, 2026

Executive summary

AI is now a board question of capital allocation, accountability and security. Boards that change how they work can create value and contain risk

Money is spent faster than its proof of value materializes

AI budgets double while only 37% of organisations report any EBIT impact (Development 1).

Autonomy and Capability are advancing faster than Control

Agents act on their own, frontier models find software flaws at scale, and trillion-parameter AI moves on-premises (Developments 2–4).

The board's own working methods are the weakest link

Directors already use AI, but few boards have rules, skills or information to govern it (Development 5).

Three questions to ask for the next 90 days

1. Request an AI value dashboard and an agent register
2. Adopt a board AI charter and a Director Skills Plan
3. Commission an AI-cyber stress test and data-class principles for AI infrastructure

No Swiss AI Act yet, but Duties apply today

Board duties

Art. 716a CO: oversight cannot be delegated. Art. 717: duty of care. Art. 754: personal liability for negligent breach.

Data protection

The revised FADP[1] covers all AI processing of personal data. The FDPIC[2] expects transparency on purpose, functioning and data sources.

Cyber reporting

Critical-infrastructure operators report attacks to the NCSC[3] within 24 hours; fines since 1 Oct 2025. Banks: 24 h, full report 72 h.

AI-specific rules

No Swiss AI Act. Council of Europe convention signed 2025; consultation draft due end-2026. The EU AI Act may reach Swiss firms serving the EU.

For SME boards: minute AI decisions, adopt a short AI policy, and watch two clocks: EU deadlines (Dec 2026 to Aug 2028) and the Swiss consultation draft (end-2026).

Sources: [7] CSA Labs; [23] [24] Swiss AI regulation; [25] Chambers (FADP, cyber); [26] [27] NCSC; [28] [29] board liability. Not legal advice.

[1] FADP stands for Federal Act on Data Protection
[2] FDPIC stands for Federal Data Protection and Information Commissioner
[3] NCSC stands for National Cyber Security Center

AI spending doubles, but profit impact lags

a What happened

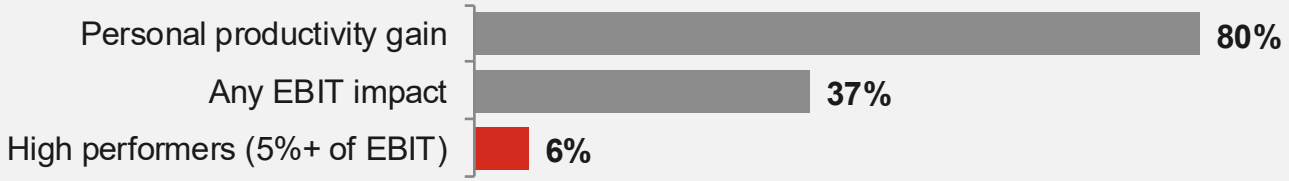
McKinsey: 80% see personal productivity gains, only 37% any EBIT impact, 6% are high performers. BCG: budgets double, and 94% of CEOs keep spending even if payoff is slow.

b Why it matters

Opportunity: high performers redesign work, not just tools.
Threat: capital flows on belief, not evidence. 82% of directors rate AI value and risk information as fair, poor or missing.

c What to do differently

- Stage-gated cases for the top 5 AI investments
- Quarterly value dashboard: EBIT, running cost, risks
- Ask: which Workflow is being redesigned and how does our Organization change?



Share of organisations (McKinsey, 2026)

SWISS LENS

34% of Swiss SMEs use AI (22% in 2024), but only 34% have rules on what data may enter AI tools. Many SMEs follow; insist on proof before scale.

Sources: [1] [2] McKinsey; [3] BCG; [14] PwC; [21] SECO / AXA-Sotomo; [22] ti&m / HSLU

Agents act, but who is accountable?

a What happened

BCG: CEOs put 30%+ of 2026 AI budgets into agents. Gartner: agents open a new attack surface; half of agent failures by 2030 will trace to weak runtime governance. EU: transparency duties applied 2 Aug 2026; high-risk rules deferred, not cancelled.

b Why it matters

Opportunity: end-to-end process redesign at scale.
Threat: decisions taken by software nobody owns, with no inventory and unclear liability.

c What to do differently

- Agent register: access, rights, owner
- Board-approved autonomy limits
- Named executive, kill-switch, incident playbook

30%+
of 2026 AI budgets go to agentic AI (BCG)

50%
of agent failures by 2030 tied to weak runtime governance (Gartner)

Dec 2027
new EU deadline for stand-alone high-risk AI (was Aug 2026)

SWISS LENS

No Swiss AI statute yet; consultation draft due end-2026. The FADP and board-liability law already apply. SMEs selling into the EU: check EU AI Act reach with counsel.

Sources: [3] BCG; [4] [5] [6] Gartner; [7] CSA Labs; [23] [24] Swiss AI regulation; [25] FADP; [28] Bratschi

AI finds flaws faster than we patch

a What happened

On 7 Apr 2026 Anthropic withheld its Claude Mythos Preview model from release and shared it with major tech and security firms (Project Glasswing). Vendor-reported: thousands of high-severity flaws, incl. in major operating systems and browsers.

b Why it matters

Opportunity: defenders can find flaws first. Threat: discovery becomes cheap and automated; legacy and OT estates are most exposed; regulators expect boards to challenge.

c What to do differently

- CISO metrics: time-to-patch, AI-assisted scanning
- Board tabletop: AI-enabled attack
- Insist on fundamentals: zero trust, segmentation
- Know your reporting duties

7 Apr

2026: model withheld from general release, shared via Project Glasswing

USD 100m

in usage credits for defensive use (vendor)

69%

of directors rank cyber and data privacy their top AI concern (PwC)

SWISS LENS

Critical-infrastructure operators must report attacks to the NCSC within 24 h (fines since Oct 2025). Ignored cyber risk can mean personal liability, Art. 754 CO.

Sources: [11] BISI; [12] Fladgate; [14] PwC; [26] [27] NCSC reporting; [28] Bratschi. Capability claims are vendor-reported.

Frontier AI can run under your desk

a What happened

NVIDIA announced DGX Station for Windows on 1 Jun 2026: 748 GB memory, 20 petaFLOPS[4], models up to 1 trillion[5] parameters and hundreds of agents run locally. Partner systems due Q4 2026; Vera Rubin data-centre platform in full production.

b Why it matters

Opportunity: highly sensitive and confidential data analyzed in-house, more sovereignty and cost control.
Threat: shadow AI with frontier power, new patching and model-provenance duties.

c What to do differently

- Classification of your data: public, not very sensitive, highly sensitive and confidential
- Hosting Cloud / hybrid / local principles by data class
- Define data that never leaves premises
- Policy for desk-side AI: owner, security, register

1 trillion

parameters: model scale that can run locally

748 GB

coherent memory in one desk-side system

Q4 2026

partner systems from Dell, HP, ASUS and others

SWISS LENS

Few SMEs are likely to buy such hardware.
Other options: the open model Apertus 1.5 (ETH, EPFL, CSCS; Apache 2.0, 24 Jul 2026) and Swiss-hosted platforms such as Swisscom's, depending on the Confidentiality of Data

Sources: [8] NVIDIA, 1 Jun 2026; [9] Enterprise DNA; [10] Techzine; [30] ETH / EPFL / CSCS; [31] EPFL / GGBA

[4] 20 petaFLOPS means 20'000'000'000'000'000 Floating Operations Per Second
[5] 1 Trillion means 1'000'000'000'000

Directors use AI, Boards lack AI Governance

a What happened

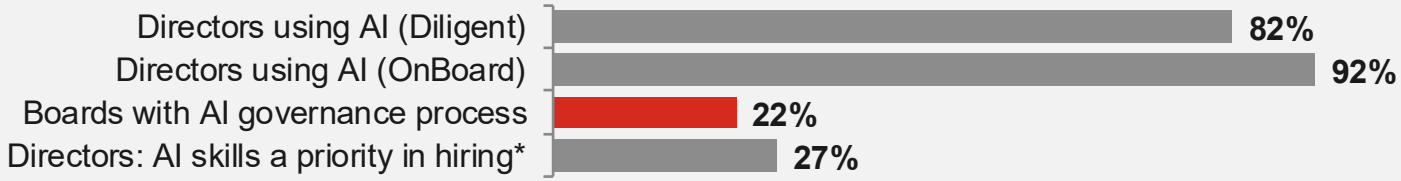
82% of surveyed US directors used generative AI for board work in six months (Diligent); 92% in OnBoard's sample. Only 22% report governance processes; 49% have heard of consumer AI tools used for board work.

b Why it matters

Opportunity: faster preparation, more time to reflect, sharper challenge of management.
Threat: confidentiality leaks and over-reliance. 71% say board AI skills must improve; only 27% weight specialist expertise in recruitment.

c What to do differently

- Board AI charter: approved tools, human-verified minutes
- AI and cyber fluency in skills matrix and evaluation
- AI as devil's advocate; accountability stays human



% of respondents, 2026 surveys. *Rate specialist expertise very important (PwC)

SWISS LENS

SME boards are small and often owner-led: a one-page AI charter, minuted AI decisions (Art. 716a / 717 CO) and one named AI sponsor would be a start

Sources: [14] PwC; [15] Diligent; [16] OnBoard; [17] Deloitte; [19] CBM; [21] SECO; [28] [29] liability. Director surveys mostly US.

Any questions for points to be clarified?

We can take 1-2 such questions now (3 mins).

If you have more or deeper questions, we can always discuss at the end.

Sharing of experiences

1. How do you use AI when preparing your Board meetings? What are your experiences?
2. What rules govern how you use AI as a board?
3. Which data would you never let leave your premises, and who decides?
4. Do you know which agents exist in your company and what they may decide alone?
5. How fast does your organization patch critical vulnerabilities, and when did the board last rehearse an AI-enabled attack?
6. Which of your AI investments can be tied to EBIT today, and which are acts of faith?

Share a concrete experience!

Sources

[1] McKinsey & Company, “The state of AI in 2026: On the road to ROI”, 25 Aug 2026 (survey of 1,719 participants, 97 countries, 4 May–8 Jun 2026). mckinsey.com
[2] McKinsey & Company, “AI is changing work. Now it has to change the organization”, 2026. mckinsey.com
[3] Boston Consulting Group, “AI Radar 2026: As AI Investments Surge, CEOs Take the Lead”, 15 Jan 2026 (2,360 executives, 640 CEOs). bcg.com. The 94% figure is as reported in press coverage of the BCG study.
[4] Gartner, “Gartner Announces Top Predictions for Data and Analytics in 2026”, press release, 11 Mar 2026. gartner.com
[5] Gartner cybersecurity predictions 2026 (A. Michaels), as reported in “Gartner: Tighten Up AI Governance or Face the Consequences”, Tech.co, 2026.
[6] Gartner Digital Workplace Summit (M. Goss), as reported in “Govern your bots carefully or chaos could ensue”, The Register, 30 Apr 2026.
[7] Cloud Security Alliance Labs, “EU AI Act’s High-Risk Deadline: Deferred, Not Cancelled”, 2026 (on Regulation (EU) 2026/1744, Digital Omnibus on AI, in force 27 Jul 2026).
[8] NVIDIA Newsroom, “NVIDIA DGX Station for Windows Puts a Trillion-Parameter AI Supercomputer on Every Enterprise Desk”, 1 Jun 2026 (GTC Taipei). nvidianews.nvidia.com
[9] Enterprise DNA, “NVIDIA Puts a Trillion-Parameter Supercomputer on Your Desk”, 2 Jun 2026 (hardware specifications and partner availability, Q4 2026).
[10] Techzine Global, “Nvidia’s plans for Vera Rubin, DGX Station, agents and robots”, Jun 2026.
[11] Bloomsbury Intelligence and Security Institute (BISI), “Claude Mythos and the Acceleration of Cybersecurity Risk”, 2026. bisi.org.uk
[12] Fladgate LLP, “Project Glasswing: what company boards need to know about Claude Mythos”, 2026 (incl. UK FCA March 2026 review).
[13] The Conversation, “Claude Mythos and Project Glasswing: why an AI superhacker has the tech world on alert”, 2026.
[14] PwC, “2026 Annual Corporate Directors Survey”, Sep 2026 (n = 561). pwc.com
[15] Diligent, “Board AI use rises: Director Confidence Index”, Jun 2026 (104 US public-company directors). diligent.com
[16] OnBoard, “2026 Board Effectiveness Survey”, sixth annual report, closed 1 Jun 2026 (531 governance professionals).
[17] Deloitte Center for Board Effectiveness, “How boards are using AI today”, Board Practices Quarterly, Jul 2026 (Society for Corporate Governance members).
[18] BDO, “2026 BDO Board Survey: Governance Under Pressure”, 2026 (200+ US public-company directors).
[19] Diligent Institute / Corporate Board Member, “What Directors Think 2026”.
[20] Harvard Law School Forum on Corporate Governance, “2026 Corporate Governance Trends to Watch” (PwC), 8 Feb 2026. corpgov.law.harvard.edu
21] Swiss SME Portal (SECO), “AI gains ground among Swiss SMEs”, 5 Nov 2025 (AXA/Sotomo labour-market study). kmu.admin.ch
[22] ti&m and Lucerne University of Applied Sciences and Arts (HSLU), “AI Maturity Study 2026”, presented 5 Feb 2026.
[23] Swiss Federal Chancellery, “Regulation of AI” (Federal Council decision of 12 Feb 2025; consultation draft due by end of 2026). bk.admin.ch
[24] Chambers Practice Guides, “Artificial Intelligence 2026: Switzerland” (Council of Europe AI Convention signed 27 Mar 2025).
[25] Chambers Practice Guides, “Cybersecurity 2026: Switzerland” (FADP and AI, FDPIC, NCSC reporting, banks).
[26] Swiss Federal Council, “Reporting cyberattacks on critical infrastructure mandatory from 1 April”, 7 Mar 2025. admin.ch
[27] Baker McKenzie, Connect On Tech, “Switzerland: Reporting cyberattacks on critical infrastructure mandatory from 1 April” (fines from 1 Oct 2025).
[28] Bratschi, “Cybersecurity und Haftung in der Schweiz” (Art. 716a, 717, 754 CO). bratschi.ch
[29] Swiss Board Forum, “Künstliche Intelligenz und persönliche Haftung: Strategische Pflichten für den Verwaltungsrat”. swissboardforum.ch
[30] ETH Zurich, EPFL and CSCS, “Apertus 1.5: Building the next generation of open AI infrastructure”, 24 Jul 2026. cscs.ch
[31] EPFL / GGBA, “Switzerland launches Apertus, a fully open multilingual large language model” (Swisscom sovereign AI platform).

Method and caveats: Sources were selected from 2026 publications by consulting firms (McKinsey, BCG, PwC, Deloitte, BDO), Gartner, NVIDIA, the Harvard Law School Forum on Corporate Governance, law firms and policy institutes. Several director surveys cover mainly US public companies and some are sponsored by board-software vendors; treat their figures as directional. Mythos-related capability claims originate from the vendor (Anthropic, the maker of Claude) and are corroborated only in part by independent commentary. Figures marked “as reported” come from press coverage of the primary study. Legal points (EU AI Act scope) should be confirmed with counsel.