RISK IN FOCUS 2026

CYBERSECURITY ROUNDTABLE – SYNTHESIS OF KEY IDEAS

A - ASSESSING THE SITUATION

Threat Level Evolution

- **Perspectives are mixed on threat escalation**. Cyber risk is rated persistently high (around 4–5/5); some industries (ex: finance) tends to see it as stable, while others (ex: manufacturing and transport) report clear escalation.
- At play: the "**cat and mouse" dynamic**. Defences improve, but attackers innovate faster, leaving organisations feeling stuck at level-4 defence against level-5 adversaries and expecting an eventual "big one".
- **Attacks increase in sophistication and collaboration**. The month-long Jaguar Land Rover SAP incident shows attackers collaborating and targeting ERP systems to maximise operational disruption.
- There is also an **intensification on sector-specific targeting**. The 2023 Danish energy case, where 15–20 organisations were breached in 24 hours through one firewall flaw, showed how one weak component can trigger near-simultaneous sector disruption.

Organisational Maturity

- It is **better than a few years ago, but still uneven**. Dedicated roles, clearer responsibilities and more cyber awareness now exist, especially in regulated sectors. Still, threat evolution outpaces maturity.
- The situation is **not the same in large or in small organizations**. Big financial institutions self-assess around 4/5 technically; smaller companies more like 3/5, but often with faster, more pragmatic recovery. A recurring paradox: high-maturity corporates with complex crisis structures sometimes react slower than small firms that "just fix it".
- **Regulation acts as accelerator but also creates distortion**. DORA, and to some extent NIS2, push penetration testing, governance and board-level dialogue. But there is concern about sliding into "compliance over risk", where checklists crowd out genuine prioritisation.

- A **technical vs organizational gap** also remains. Cyber teams may be level 3–4, but enterprise-wide crisis management and business continuity are closer to 1.5–2/5. Exercising playbooks, clarifying decision rights and cross-functional coordination lag behind.

Resource Allocation and Workforce

- **Audit dedication ranges from 25% to 70%.** Some smaller financial institutions spend 60–70% of internal audit effort on cyber and IT; many other sectors sit around 25–33%, depending on whether fraud is counted.
- **Headcounts are stable, yet workload is growing**. Cyber scope expands (cloud, AI, third parties), but audit teams rarely grow proportionally. Organisations compensate by relying on second-line testing, external specialists and shared assessments.
- The **skills shortage remains structural**. Hiring hybrid profiles (e.g., ex-pen-testers who also understand Information Security Management System and regulation) is extremely difficult; many roles are filled by upskilling internal staff or buying expertise from the market.
- **Many leans on the second line**. Where strong CSO functions exist (e.g., 10–12 cyber specialists in a small group), they perform deep technical testing, while internal audit focuses on methodology, governance and validating second-line work rather than duplicating it.

B - THREAT LANDSCAPE

AI-Related Threats

- **Deepfakes and voice cloning cases are growing**. Cases include a deepfake video/voice of a senior executive on an internal Teams call, attempting to authorise urgent payments. One incident at a Nordic bank was blocked only because staff in Singapore questioned the request, highlighting cultural and process factors as defences.
- **Shadow AI is also a growing problem**. Staff freely use public AI tools to be more productive. Proxy logs show significant traffic to external models, but not the content, creating silent data-exfiltration risk. Simply banning AI is seen as unrealistic; without sanctioned tools, shadow AI will flourish.
- **Governance struggles**. Organisations are building AI registers and risk classifications but are constantly catching up: SaaS vendors add AI features “sideways”, and developers experiment with models in code repositories. Identifying “critical/high-risk AI” versus low-risk use remains hard.

- The **new AI is also fragile**. The Model Context Protocol (MCP) is compared to early Wi-Fi – powerful connectivity with little embedded security, enabling prompt-injection-like attacks. Controls must be layered on top: role-based access, guardrails, and strict control of what agents can reach.
- **Fraud scales up.** AI makes fake photos, receipts and narratives cheaper and more convincing, pushing insurers and banks to use AI for anomaly detection just to keep fraud levels manageable.
- **And how about offensive AI?** It is feared but not yet dominant. Participants haven't clearly seen "AI-powered autonomous hacking" but assume it's coming; they worry about over-investing in hypothetical future scenarios vs today's very real ransomware and phishing.

Geopolitical Threats and Cyber

- **Geopolitics is explicitly built into cyber risk (for some).** Nordic and large organisations, often led by CSOs with military-intelligence backgrounds, link hybrid warfare and cyber. They track Russia, China, Iran and others in formal analyses.
- Country-based vendor and access scrutiny:
    - **Russia:** primary hostile actor in many threat models; some firms exited Russia after the Ukraine invasion, closing plants and sales.
    - **China:** concerns around surveillance and state access; organisations note attacks aligned with Chinese working hours and may avoid placing Chinese nationals in highly privileged roles.
    - **India:** emerging risk due to data-access rules and perceived intelligence collaboration with Russia, especially for sensitive personal data.
    - **US:** fear that future administrations could "weaponise" US-based cloud providers, prompting questions about real exit capability from hyperscalers.
- **Selective hiring for critical roles is developing**. In some jurisdictions, it is now legally permissible to exclude nationals from specific countries from high-privilege security and audit roles. This reduces some risk, but participants describe it as ethically uncomfortable.
- **Cloud risks lead to thinking about cloud sovereignty and exits**. To keep options open, organisations containerise workloads and, in some cases, run Azure-type services on-premises. They accept losing some advanced features in exchange for geopolitical resilience.
- Also on the radar: **Hybrid threats to infrastructure.** Submarine cables, key fibre junctions, airports and ports feature in scenario planning; drone incidents at critical nodes are seen as part of a broader hybrid warfare toolkit.
- Yet – **for smaller firms: they are all just "bad guys".** Without threat-intel capacity, smaller organisations don't differentiate between criminal and state attackers; they focus on hygiene and response rather than attribution.

Evolution of Cyber Criminality

- **Collaboration expands among attackers**. APT-style groups share exploits and techniques, accelerating spread of successful attack patterns.
- **MFA is necessary, but not sufficient**. MFA still blocks many attacks but can be bypassed; awareness and layered controls are essential to prevent session hijacking or social-engineering-driven approvals.
- **Ransomware moves into OT** [Operational Technology, in use in the factory; different from IT for the office]. Poor segmentation lets attackers jump from IT to operational technology. The Jaguar Land Rover outage is a vivid example of how impacting ERP/production-orchestration systems can freeze manufacturing globally.

C - PREPARING FOR THE THREATS

Resilience and Post-Breach Protection

- **Crisis management is the weak link**. Across sectors, participants rate technical security above organisational crisis readiness. NIS2 and DORA are now forcing more structured crisis management and continuity planning.
- **Board-level awareness is critical**. Professional bodies issue board-oriented guidance on cyber, legal duties and crisis management. Yet auditors say the "window of opportunity" to engage boards is tiny – timing and framing are critical.
- **Risk appetite must be made concrete**. Mature firms run simulations with their executive teams: "At what point do we declare a crisis? When claims cannot be processed? When sales stop? When trading or investments are impaired?" This translates abstract appetite into operational thresholds.
- **Backups constitute an existential safeguard**. The nightmare scenario is a single attack corrupting both production and backups. This drives interest in segmented, offline and immutable backups.
- **Smaller firms may demonstrate higher agility**. Smaller organisations, despite weaker technical controls, often excel at business continuity: decision chains are short and people can improvise quickly to restore operations.

AI in Cybersecurity Defence

- **AI can be used for audit and detection** – but sequence matters. Some internal audit teams first learned how to audit AI models before using AI to speed up their own work. On the defence side, AI-enhanced tools support faster scanning and patching, especially in cloud environments.
- What also matters: **Shadow AI monitoring**. Techniques include: proxy logs to see who is calling public models, code scanning for embedded models, and specific review of SaaS vendors silently adding AI features.

- On **fraud analytics**, Insurers and banks can deploy AI to spot anomalous claims or transactions, effectively entering an "AI vs AI" arms race with fraudsters.

Cyber Talent Management

- **Shortage won't disappear**. Participants don't expect a future where skilled cyber people are abundant. Instead, they plan around permanent scarcity.
- **Competency matrices matter**. Under DORA, firms document the skills needed across infrastructure, development, mainframe and red-team, highlighting gaps and guiding recruiting and training.
- **At stake: Upskilling and collaboration**. With hiring bottlenecks, organisations invest in training existing staff and rely on collaborative models like the Cloud Collaborative Audit Group (around 65 members), which conducts joint audits of hyperscalers and key SaaS providers.
- **Audit vs first/second line skills?** Many organisations accept that very deep technical expertise will sit in first/second line. Internal audit focuses on evaluating governance, methodology and the quality of second-line testing.

Top Management Awareness and Investment

- **Board awareness is today significantly better**. Cyber is now a recurring board topic, driven by regulation and by high-profile incidents. Crisis exercises are increasingly used to make impacts tangible.
- **Yet, cyber competes with other big risks**. Geopolitics, macro-economics and cost pressures also weigh heavily. Some participants question whether cyber always deserves the top-risk position vs being one of several strategic threats.
- **The Second-line is also strengthening**. Many companies have doubled second-line cyber capacity; even small groups may employ 10–12 specialists. IT functions also invest heavily in vulnerability identification and remediation.
- **However, there is still a "quantification gap".** Although everyone talks about cyber-risk quantification, most investment decisions remain based on regulatory drivers and qualitative judgement rather than robust monetary models.

Governance Challenges

- **Access control is a critical enabler**. Tightening local admin rights and privilege management slows the spread of unapproved tools and reduces attack surfaces.
- **Ban vs enable re AI?** Participants converge on a key insight: pure prohibition drives shadow AI. The preferred approach is to provide secure, powerful internal or enterprise AI solutions so employees aren't tempted to use uncontrolled public tools.
- **Some organisations deploy their own LLMs** – "offline" or sandboxed versions – and pair them with enterprise tools like Copilot, gaining productivity while keeping data inside controlled environments.

- Overall, **asset and tool discovery should be expanded**. Automated scanning is used to maintain inventories and identify shadow IT/AI, particularly in developer environments and SaaS portfolios. Organizations must strive to define which AI tools are allowed, especially in API-heavy environments, and back this with scanning for unapproved tools.
- Beyond, **third-party risk intensifies**. More SaaS, more AI inside vendors' products, and opaque sub-supplier chains amplify dependency risk. Many fear vendors may process sensitive data with AI features that customers have neither approved nor assessed.

D - ON THE HORIZON – WHAT KEEPS AUDITORS AWAKE

- **Growing risk: Production and backups hit together**. A single attack encrypting or corrupting both live systems and backups is the scenario many fear most, because it moves from "serious incident" to "existential event".
- **AI's provides promises & unknown risks**. There is excitement about efficiency gains and equal concern about the "unknown unknowns" AI may introduce. Leaders worry about betting too hard either for or against rapid AI adoption.
- **The networked corporation creates third-party explosion**. Expanding ecosystems of vendors and sub-vendors create a sense of systemic fragility that is hard to map, let alone audit comprehensively.
- **What still is missing: budget!** Many would like "double the staff" or "more budget, more people, more time". Demand from boards and management outstrips capacity; each new request tends to become a large exercise.
- **Yet, it's not only about mone**y but the way to reshape culture, skills and people competencies.
    - **Shifting management thinking** and everyday behaviour is consistently described as harder than deploying tools. Human factors – awareness, skills, priorities – are the most stubborn vulnerabilities.
    - **Reskilling preoccupies also Internal audit**, that worries about having enough technical depth to credibly challenge first and second line, particularly on complex cloud and AI topics.
    - Ultimately, **most serious failures are seen as rooted in people** – insufficient competence, poor decisions, or weak culture – rather than purely technical gaps.

***Roundtable contributors**: Gaute Brynildsen, Ibtissam Doha, Luca Mario Antonio Laguardia, Orjan Martensson, Gerhard Schreihans, Meike Siebert, Roul Vierke and John Wallhoff*.

Conversations facilitated by Guy-Philippe Goldstein.