Tunku Mahmood Fawzy (Tunku Kecil Muda) Tunku Muhiyiddin

He/Him

Independent Non-Executive Director | Strategic Judgement | Institutional Stewardship | Crisis Leadership | FCMA | MBA (Warwick)

HSBC

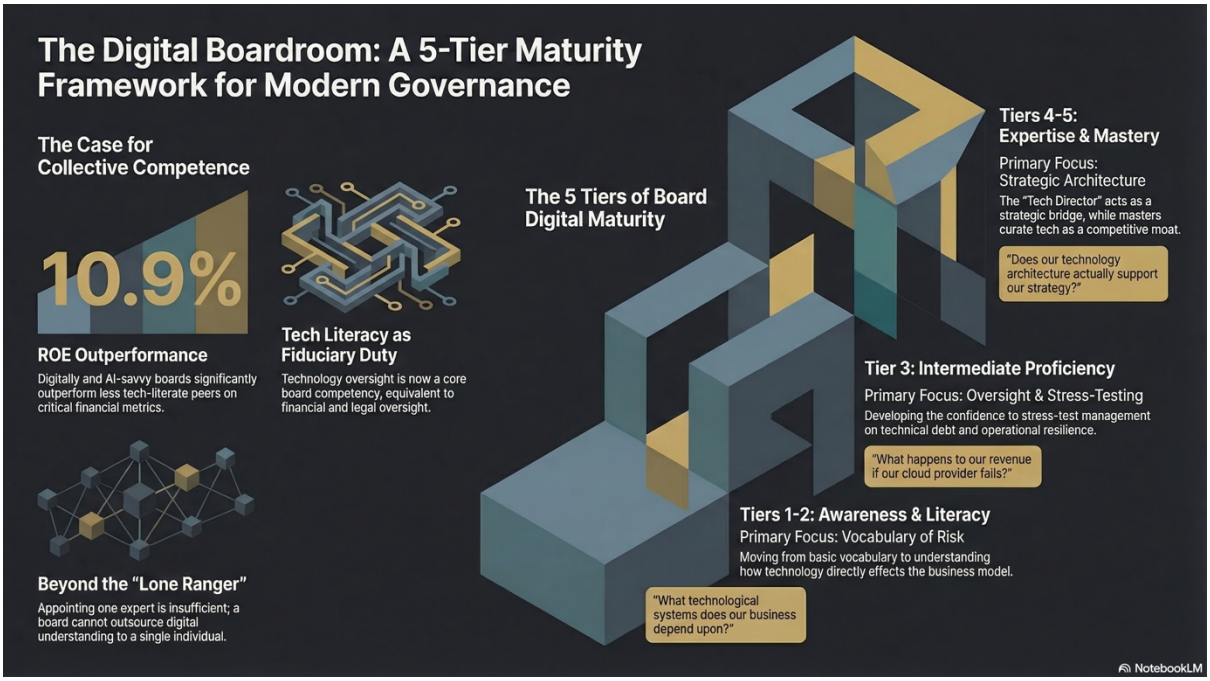
University of Warwick - Warwick Business School

Stewardship is the disciplined guardianship of institutions we neither own nor will outlive. It is grounded in ethical conduct and fairness — irrespective of reciprocity — and anchored in prudential judgment, common sense, and alertness to changing conditions. Stewardship requires a strategic outlook tempered by sustainability: the capacity to endure rather than chase immediate advantage. It recognises that we are temporary custodians of enduring structures, responsible for strengthening rather than exploiting them. To steward is to leave an institution structurally stronger than we found it, preserving its integrity, continuity, and ability to withstand uncertainty, volatility, and danger. Institutions endure through stewardship, not disruption.

Tunku Dato' Seri Mahmood Fawzy 2026

2026-03-18

Digital Literacy in the Boardroom



Introduction

In 2026, the business world faces a period of unprecedented uncertainty and transformation. Geopolitical, environmental, and technological challenges are threatening global stability. For the modern corporation, technology is no longer an operational layer or a siloed department; it has become the **nervous system of the enterprise**. Decisions regarding software infrastructure, cloud platforms, and artificial intelligence (AI) now determine capital allocation, operational resilience, and competitive positioning. The BNM RMiT 2025 is explicit in detailing the requirement for a technology director for financial institutions but is that enough?

Despite this reality, many boards remain unprepared. Research indicates that 80% of Independent non-executive directors believe their current structures are inadequate for AI oversight, and 67% feel the same about rapidly evolving cyber risks. Furthermore, 40% of CIOs rate their boards' effectiveness as "poor," citing a persistent knowledge gap in digital transformation. To secure the future, boards must move beyond "wishful thinking" and embrace **digital literacy as a fiduciary competence**.

The Fiduciary Imperative for Technology Oversight

Historically, board competence revolved around finance, legal oversight, and industry knowledge. However, technology innovations have transformed almost every business strategy and process, bringing new, hard-to-quantify risks. Cybersecurity threats, ranging from state-sponsored organizations to lone hackers, represent an increasing and evolving threat to all businesses.

Board members have fiduciary duties to act in good faith, care, and loyalty. Just as boards are expected to oversee financial risks, they must now engage in **high-level oversight of systems, controls, and management activities** that address technological vulnerabilities. The legal standards for director liability are high, but precedents like the *Caremark* and *Stone* decisions make clear that directors cannot simply ignore their risk oversight responsibilities. Shareholders are increasingly holding directors accountable for cybersecurity failings, with lawsuits often alleging that boards failed to implement effective programs or ignored "red flags".

Defining the "Tech Director"

Many boards make the mistake of assuming any "tech person" will suffice. However, a "tech director" is not merely someone who has worked in IT or can write code. A proper definition must start with the board's duty: a Tech Director is a member capable of providing **independent oversight of technology strategy, risk, and digital resilience**, and able to challenge management on technology-related decisions that affect enterprise value.

A competent Tech Director possesses four essential forms of competence:

1. **Technology Governance Literacy:** Understanding how technology is governed, including enterprise architecture, risk frameworks, and third-party dependencies.
2. **Ability to Challenge Strategy:** Interrogating management on cloud migration, AI adoption, data governance, and vendor (Cloud) concentration risk or Nth vendor vulnerabilities.
3. **Cyber and Operational Resilience Awareness:** Interpreting cyber briefings, incident simulations, and resilience metrics to understand how failures could create enterprise-level crises.
4. **Understanding of Technology Economics:** Treating technology as a strategic capital deployment rather than mere "IT spend," including "build vs. buy" decisions and software lifecycle costs.

The Board Digital Competence Model

The goal of a modern board is **collective capability**, not a single expert. Boards often fail when they appoint one expert and then defer all technology-related decisions to that individual, creating a "knowledge silo". Instead, the entire board must possess a baseline level of digital literacy.

The following five-tier model defines the levels of competency required for effective governance:

- **Level 1: Fundamental Awareness (Novice)** Directors at this level understand the vocabulary of digital risk (e.g., cloud computing, data governance, AI). They recognize basic concepts and their strategic relevance but lack technical detail. This awareness prevents the boardroom from being blinded by technical jargon.
- **Level 2: Working Knowledge** These directors understand how technology affects the business model, including digital transformation programs and technology supply chains. They can ask practical questions about system dependencies and the consequences of system failures.
- **Level 3: Intermediate / Proficient** Directors at this level can interpret technology governance information. They can evaluate cyber risk reports, assess the feasibility of digital roadmaps, and challenge management assumptions about cloud strategies or AI deployment.
- **Level 4: Advanced / Expert (The Tech Director)** This level represents the specialist. They possess deep experience in enterprise architecture, cybersecurity leadership, or large-scale digital platforms. They translate technical issues into strategic implications and raise the literacy of the entire board.
- **Level 5: Mastery (Solution Curator)** Mastery involves understanding how technology reshapes entire industries and anticipating the economic implications of emerging ecosystems. These individuals curate technological solutions at the level of corporate strategy.

The Ideal Board Composition

To ensure rigorous oversight, boards should aim for a balanced distribution of these competencies. A healthy board composition typically follows this structure:

- **Novice (20–30%):** Must speak the vocabulary of digital risk.
- **Working Knowledge (30–40%):** Understands how tech drives the business model.
- **Intermediate (20–30%):** Can actually stress-test management.
- **Advanced (1–2 directors):** The "Tech Director" bridge-builders.
- **Mastery (Rare):** Strategic visionaries who curate future solutions.

By ensuring that no director remains technologically illiterate, the board's collective capability is elevated, making management briefings more transparent and strategic decisions more informed. The gold standard.

How to Find a Tech Director

Finding the right Tech Director often requires searching outside traditional networks. Boards can and should proactively seek candidates with strong backgrounds in technology, such as executives from tech companies or experts in digital transformation.

Four genuine archetypes of effective tech directors include:

1. **Former Enterprise CIO / CTO:** Experienced in running large-scale systems in complex organizations.
2. **Cybersecurity Leader:** Deeply understands digital threat landscapes and resilience.

3. **Digital Platform Strategist:** Experienced in building digital products or AI-driven businesses.
4. **Technology Risk / Infrastructure Specialist:** Familiar with resilience engineering, cloud architecture, and financial system technology.

Organizations can leverage **executive search firms** to identify these candidates, a significant number of companies now use these search firms to find technology expertise. Additionally, networking outside the tech world and speaking with executive search consultants can help identify unique candidates who possess both technical depth and governance capability, but honestly it is like gold dust.

Bridging the Competency Gap

Upskilling the board is a continuous journey rather than a one-time exercise. Boards can use several practical tools and strategies to bridge the literacy gap:

- **Board Technology Skills Matrix:** An editable grid mapping director expertise against the skills needed (e.g., AI, data privacy) to visualize strengths and identify gaps for recruitment or training.
- **Director Self-Assessments:** Questionnaires that allow directors to privately identify areas where they need to deepen their understanding.
- **Regular Education Sessions:** Organizing workshops, site visits, and "tech deep dives" featuring internal and external experts to highlight current industry and regulatory topics.
- **War Games and Drills:** Participating in board-level cyber incident simulations to understand crisis escalation structures and recovery objectives.
- **Leveraging External Advisors:** Using technology consultants or ad hoc advisory committees to provide fresh perspectives and evaluate the company's programs.

Conclusion: Technology as Stewardship

Technology governance is now a core board competency. Boards are no longer just monitors of financial performance; they are **stewards of institutional resilience**. As regulators and investors increasingly focus on cyber resilience and technology risk, a board's technological understanding becomes a source of strategic competitive advantage.

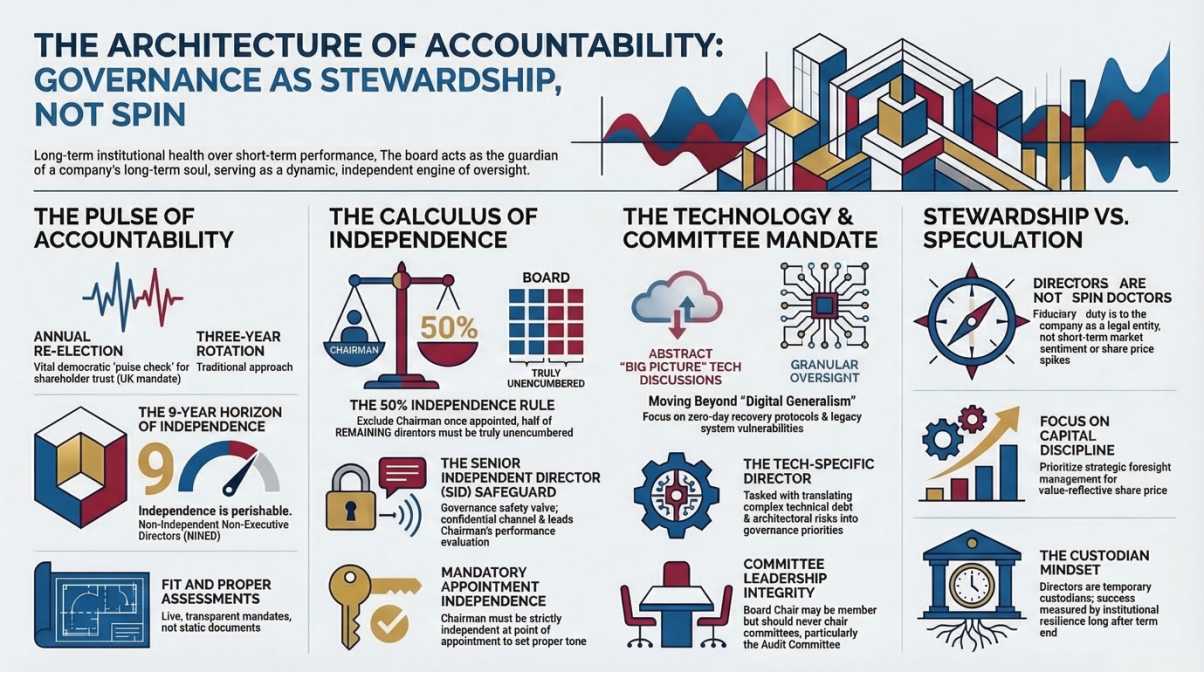
The board of the future will not belong to the one with the single smartest technologist, but to the board where **every director understands the digital world well enough to govern it wisely**. Enhancing effectiveness is the most critical step to securing a company's future in the complex risk environment of 2026 and no, it is not being savvy about "disruption".

2026-03-18

2026-03-18

Article Title: The Architecture of Accountability: Why Boards Must Prioritize Stewardship and Avoid Corporate Spin!

Summary Effective corporate governance is increasingly defined by the transition from mere procedural compliance to a deep-seated culture of stewardship. In an era of heightened volatility, boards must act as the guardians of a company's long-term soul rather than the architects of short-term share price movements. This comprehensive exploration of modern board architecture examines the structural pillars of accountability, ranging from the necessity of annual director re-elections to the "calculus of independence" regarding the Board Chair. It highlights the critical role of the Senior Independent Director as a governance safety valve and argues that boards must develop granular technological competence to manage systemic cyber risks. Furthermore, it reinforces that director independence is a perishable commodity, advocating for a strict nine-year tenure limit to ensure fresh perspectives. Ultimately, governance is about the disciplined oversight of institutions that must endure beyond any individual term, prioritizing integrity and long-term resilience over market spin.



The Architecture of Accountability: Stewardship Over Procedural Compliance

In the evolving global landscape of corporate governance, a perennial tension exists between "form" and "substance". Too often, governance reform is misunderstood and treated as a mere technical exercise involving more rules, more disclosures, and more procedural obligations. However, the reality is that effective governance rarely emerges from the proliferation of rules alone. Instead, it emerges from a clarity of roles, balanced power

structures within the boardroom, and a culture of stewardship that guides how those structures are used.

The pendulum of modern oversight is swinging decisively toward a fundamental truth: the board is the guardian of the company's long-term soul, not the architect of its short-term share price. To remain resilient in an era of unprecedented volatility, boards must move beyond "compliance theatre" and examine the structural pillars that ensure a board is fit for purpose. This shift requires a disciplined oversight of institutions that must endure beyond the tenure of any individual director. Directors are not owners; they are temporary custodians entrusted with safeguarding long-term enterprise value on behalf of shareholders and society.

The Pulse of Accountability: Rethinking Annual Re-election

One of the most visible governance practices in developed markets is the annual re-election of directors, which serves as a vital pulse check of shareholder trust. In the United Kingdom, the Corporate Governance Code mandates that all directors of FTSE 350 companies stand for annual re-election. This reinforces the essential principle that board positions are not entitlements but responsibilities subject to continuing shareholder confidence. Each year, shareholders are given the opportunity to express that confidence or withdraw it.

In Malaysia, the standard practice has traditionally remained a three-year rotation, the "one-third" rule. While the rotation model provides stability, it is worth asking if it provides sufficient accountability for the modern era. In a context where ownership is concentrated and where large Public Interest Entities (PIEs) are prevalent, annual re-election can serve as a vital democratic pressure valve. For "Large Companies" such as those in the FBM 100 or PIEs annual re-election should not be viewed as an administrative burden but as a meaningful mechanism of accountability. When a director stands for re-election annually, the "fit and proper" assessment ceases to be a static document hidden in a filing cabinet; it becomes a live, transparent mandate. For smaller listed companies, the traditional rotational system may remain appropriate, as the objective should be thoughtful proportionality rather than rigid uniformity. The "fit and proper" assessment should be robust supported with detailed background checks from credible service providers.

The Independence of the Chairman: A Strategic Calculus

Few positions shape the tone and effectiveness of a board more profoundly than the office of the Chairman. Across most governance frameworks and jurisdictions, it is widely accepted that a Chairman must be independent at the point of appointment. However, there is a profound nuance in the "Independence Calculus" that is often misunderstood. Once appointed, the Chairman occupies a role fundamentally different from other non-executive directors; they set the board agenda, shape boardroom culture, and manage the flow of information between directors and management.

The UK Code recognizes this reality by excluding the Chairman from the "independence count" of the board once they have taken the gavel. The logic is grounded in the fact that a Chair is the chief architect of the board's culture and the primary interface with the CEO, meaning they are no longer a neutral observer. Counting the Chair as an Independent Non-Executive Director (INED) in the 50% requirement can mathematically overstate the board's true level of independent challenge. By excluding the Chair from this calculus, a more robust board composition is forced, ensuring that at least half of the remaining directors are truly

unencumbered by the internal dynamics of board leadership. Governance should not rely on the appearance of independence; it must ensure independence in substance.

The Senior Independent Director: The Board's Internal Counterbalance

Even with an independent Chairman, the architecture of a high-performing board is incomplete without a Senior Independent Director (SID). The SID performs an essential balancing function and acts as a governance safety valve. First, the SID acts as a sounding board for the Chairman, providing an alternative perspective on board dynamics. Second, the SID provides a confidential channel for other directors to voice concerns where they believe matters cannot be comfortably addressed through conventional board processes. Third, the SID offers shareholders a direct line of communication, particularly when concerns involve the Chairman or the broader leadership of the company.

In the Malaysian context, the SID's role is particularly critical in three scenarios: where policy and profit lines can blur, founder-controlled firms where the Chair may have deep historical ties, and dominant shareholder environments where minority interests require a dedicated champion. The SID also leads the annual evaluation of the Chairman's performance. Without an SID, independent directors may feel they have no "neutral ground" to discuss board leadership. These functions are not ceremonial; they ensure that boards retain internal mechanisms for challenge and reflection, preventing an excessive concentration of influence.

Stewardship vs. Speculation: Directors Are Not Share-Price Managers

A dangerous trend in modern capital markets is the expectation that directors should drive share prices. However, this is not, and should never be, the role of a director. A director's primary fiduciary duty is to the company as a legal entity, which translates to the pursuit of long-term sustainable success. Share prices are market outcomes shaped by macroeconomic conditions, investor expectations, and liquidity dynamics—they are not instruments that boards should attempt to manage.

When boards become overly preoccupied with short-term share price performance, distortions often follow. Strategic investment may be delayed to protect quarterly earnings optics, and long-term innovation may be sacrificed to maintain near-term investor sentiment. Shareholders do not need directors to manage market mood or engineer short-term price spikes; they need them to exercise capital discipline, strategic foresight, and risk management. If the board ensures the company is well-governed and the strategy is executed with integrity, a value-reflective share price will follow as a consequence over time.

Board Committees: Membership without Dominance

The committees of the board Audit, Nomination, Remuneration, and Risk (in rare cases you may have a Technical Committee) are the engine rooms of governance where the heavy lifting is done. To maintain their integrity, the leadership structure must remain pristine. Committee leadership should remain firmly in the hands of independent directors, and the Board Chair should never chair these committees. While it is often permissible for the Board Chair to be a member of certain committees to provide context and insight, safeguards must remain clear.

As always every committee must maintain a majority of Independent NEDs to ensure that the "check and balance" remains functional. Specifically, in the Audit Committee, the Board Chair should ideally not even be a member to ensure total separation between board leadership and financial oversight. In any committee where they sit as a member, the Chair must be willing to recuse themselves when their presence might stifle independent debate or where conflicts of interest arise. Power must never accumulate unchecked within any single office.

The Technological Mandate and Cyber Resilience

In the digital age, technology is no longer a peripheral issue; it sits at the centre of operational resilience and competitive advantage. For too long, boards have viewed technology through a purely "strategic" lens, treating it as a broad theme for annual retreats. This approach is no longer sufficient, as cyber-attacks and system failures can cripple institutions within hours. Board-level discussions must move from the abstract to the granular, ***it is not enough to say that technology is disruptive.***

It is no longer enough to ask, "Are we digital?"; the board must ask precise questions about system architecture, data exfiltrated zero-day recovery protocols, and legacy system vulnerabilities. To achieve this, the era of the "generalist board" must evolve. **At least one director should be specifically tasked with maintaining a working familiarity with the organization's technological landscape and cyber posture**. This director serves as the bridge, translating complex technical architectural risks into governance priorities. Without such granular capability, the board is effectively flying blind in a digital storm, and technology oversight risks becoming superficial. Technological literacy has become a core governance competency. Much has been written elsewhere and boards can use the foundations of NIST and ISO/IEC to anchor the technology component.

The Nine-Year Horizon: The Perishability of Independence

Independence is not a permanent attribute; it is a perishable commodity. Over a long enough timeline, even the most rigorous director can fall victim to "familiarity threat," where years of shared decisions and relationships soften the edge of independent challenge. For this reason, it is prudent to recognize nine years as the natural horizon of independent directorship.

Beyond this nine-year point, a director’s psychological independence is naturally diminished. While their wisdom and institutional memory remain invaluable, they should transition to a Non-Independent Non-Executive Director (NINED) role if the board and shareholders believe their experience remains valuable. Falsely labelling a long-tenured director as "independent" does a disservice to the market and undermines the credibility of the independence status. A clear "nine-and-out" rule for independence status forces a cycle of healthy refreshment, ensuring that the boardroom is constantly challenged by new perspectives and diverse eyes that are not anchored in the decisions of the past decade.

Granted that a four year “INED” may have already been “captured” and a nine year outgoing INED may be more than happy to question and challenge management but there should be no exceptions, and if the entity wishes for the individual to continue, they can do so as NINEDs,

Conclusion: The Custodians of the Future

Ultimately, corporate governance is not about the quarterly report or managing appearances; it is about the next decade and the long-term health of the institution. The tools of modern governance from granular technology oversight to the arithmetic of independent chairmanship are structural safeguards that allow a board to fulfil its true purpose: stewardship.

Directors are the temporary custodians of enduring institutions, and their legacy is not measured by daily share price fluctuations but by the resilience, integrity, and sustainability of the companies they leave behind. This requires the courage to resist short-term market pressures and the discipline to maintain an architecture that prioritizes integrity over "spin". Good governance begins with the premise that boards must act not as owners, but as stewards who ensure the institutions they lead emerge stronger than when they were first inherited. Institutions endure not because of rules alone, but because the people entrusted with them exercise judgment, restraint, and responsibility.

2026-03-14

AI Governance 2026: From Hype to Supervised Reality

The year 2025 marked a decisive transition in AI governance, moving from abstract principles to real-world enforcement and operational constraints. As we head into Q2 2026, the question is no longer whether governance frameworks exist, but whether they are robust enough to withstand legal scrutiny and significant financial ramifications. The rest of **2026 is the year these new expectations will be tested**,

particularly as enterprises move beyond simple "copilots" toward **agentic AI** capable of executing autonomous actions.

To navigate this landscape, leaders must bridge the gap between high-level regulatory mandates and the actionable guidance needed for practical implementation. This article provides a comprehensive roadmap for 2026, focusing on the **12 Key Accountability Questions**, the latest **NIST and ISO frameworks**, and the looming deadlines of the **EU AI Act**.

The 12 Questions: Turning Principles into Accountability

High-level principles like "fairness" and "transparency" are necessary but often too abstract to audit. In 2026, regulators expect an "operating model" rather than a static policy. The following 12 questions serve as a checklist to force evidence, define owners, and create a traceable audit trail for AI systems:

1. **Purpose & Materiality:** What specific decision is the AI influencing (e.g., marketing, credit scoring, or clinical triage), and how central is it to your business?
2. **Client & Societal Impact:** Who can be harmed by this system, and what is the nature of that harm (e.g., financial loss, denial of service, or discrimination)?
3. **Data Provenance & Consent:** Where did the training data originate, are you legally permitted to use it, and can you prove it to an auditor?
4. **Bias & Fairness Testing:** Has the model been tested for disparate impact across specific segments rather than just broad averages?
5. **Robustness & Stress Testing:** How does the system behave during "regime shifts," tail events, or intentional adversarial attacks?
6. **Explainability Appropriate to Risk:** Can the system provide a justification for its outputs that is sufficient to support an appeal or a counter-factual explanation (e.g., LIME or SHAP values)?
7. **Human Override & Escalation:** Who has the authority to stop a trade, block a clinical decision, or revert a system action in real-time?
8. **Security & Resilience:** Are there protections in place for the entire data pipeline, the model weights, and the prompt interface?

9. **Vendor & Outsourcing Controls:** Do your third-party contracts include audit rights, SLAs, and mandatory update notifications?
10. **Monitoring Metrics:** Are you tracking concept drift, override rates, and incident reports post-deployment?
11. **Governance & RACI:** Are there named accountable executives and a "three lines of defence" model (operational, oversight, and audit)?
12. **Disclosure & Communications:** Are users clearly informed when they are interacting with an AI, and is the system's purpose accurately described without "AI-washing"?

The 2026 Framework Landscape: NIST and ISO

In 2026, voluntary frameworks are becoming the "de facto" benchmarks for compliance, even in non-regulated sectors.

NIST AI Risk Management Framework (AI RMF) 1.0

NIST's framework remains the gold standard for managing AI risks. It is built around four core functions:

- **Govern:** Establishing a culture of risk management and clear accountability.
- **Map:** Identifying the context and risks associated with specific AI use cases.
- **Measure:** Employing quantitative and qualitative tools to analyze and track identified risks.
- **Manage:** Implementing prioritized risk responses based on the organization's risk tolerance.

The New NIST Cybersecurity AI Profile (December 2025 Draft)

As we enter 2026, cybersecurity programs must integrate the unique realities of AI advancements. The new NIST profile focuses on three areas:

- **Secure:** Managing cybersecurity challenges for any AI system.
- **Defend:** Using AI to improve organizational cybersecurity defenses.
- **Thwart:** Building resilience against AI-enabled threats like automated phishing or data poisoning.

ISO/IEC 42001: The AI Management System

This is the first global standard for AI governance. It requires organizations to establish formal roles, continuous improvement loops, and specific risk processes for every stage of the AI lifecycle. Unlike broad principles, ISO/IEC 42001 provides a structured pathway for third-party certification, which is becoming a critical "hero" indicator for business-to-business trust in 2026.

The EU AI Act: 2026 Milestones and the "Digital Omnibus"

The EU AI Act is currently in its phased implementation period, with **August 2026** serving as a pivotal milestone.

- **GPAI Models:** As of August 2025, obligations for general-purpose AI (GPAI) foundation models are already active, requiring providers to publish summaries of training data.
- **Prohibited Practices:** Bans on "unacceptable risk" practices (e.g., social scoring) took effect in early 2025.
- **Transparency Rules (August 2, 2026):** Specific disclosure obligations will come into force. For instance, chatbots must be identified as machines, and "deep fakes" or AI-generated text published to inform the public must be clearly labeled.
- **High-Risk AI Systems (The "Digital Omnibus" Shift):** Originally, the bulk of obligations for **Annex III High-Risk AI** (e.g., AI used in recruitment, education, or critical infrastructure) was due on August 2, 2026. However, due to delays in technical standards, the European Commission proposed the **Digital Omnibus on AI Regulation**.

Key Timeline Updates (Proposed):

- **Annex III High-Risk Systems:** The deadline may be postponed to **December 2, 2027**, or six months after the Commission confirms adequate compliance support is available.
- **Annex I (Embedded) Systems:** These systems (e.g., AI in medical devices or vehicles) have a proposed backstop deadline of **December 2, 2028**.

Critical Issues for 2026: Agentic AI and Auditability

While the regulatory timeline shifts, the technology is accelerating. Two major governance gaps have emerged that leaders must address immediately:

1. From Model Outputs to System Actions

Traditional AI risk focused on biased responses or hallucinations. In 2026, the focus has shifted to **agentic AI actions**. When a clinical AI prioritizes one patient over another or a financial agent initiates a transaction, liability centers on the **action** taken with limited human oversight. Governance must move to "runtime," including **real-time monitoring** and automated guardrails that can stop a system when it deviates from expected behavior.

2. The "Shadow AI" Inventory

Organizations are discovering they use AI in far more places than formally approved—often through employee-led experimentation or embedded SaaS features. In 2026, the expectation is for **granular and operational governance**. This includes maintaining an accurate AI inventory, documenting model lineage, and assessing third-party vendors with the same rigor as internal systems.

The "Sharp Edges": Liability and Systemic Risk

As we refine our approach, we must address the "fault lines" where legal and insurance battles are being waged in 2026.

Liability Architecture: Who Pays When it Breaks?

2026 is the year the insurance industry starts demanding very specific answers before writing a policy.

- **Product Liability vs. Negligence:** With the **EU Product Liability Directive (PLD)** now classifying AI as a "product," the burden has shifted. Claimants may only need to prove a defect, not negligence. However, if a user provides a reckless instruction to an otherwise safe agent, the liability shifts back to **professional negligence**.
- **Insurance Prerequisites:** Insurers now require **"Evidence of Intent" logs** to distinguish between software failure and human misuse.

The "N-th" Party Exposure (Recursive Risk)

The supply chain is no longer linear; it's recursive. Your 3rd-party SaaS vendor likely relies on a 4th-party LLM, which uses a 5th-party vector database.

- **Visibility:** A failure at the 5th level can collapse your entire workflow. 2026 governance mandates **AI Bills of Materials (AIBOMs)** to map these hidden dependencies.

Militarized AI & Reckless Negligence

In high-stakes environments, the "meaningful human in the loop" is no longer just a best practice—it's a legal shield.

- **Automation Bias:** Relying on AI for lethal or high-impact decisions without independent verification is increasingly viewed as **reckless negligence**. International norms are crystallizing around the principle that human primacy must be preserved in critical decision cycles.

Cloud Service Providers (CSPs) as Targets

CSPs are now the **Systemic Brain** of the global economy.

- **Concentration Risk:** Consolidation on a few hyperscalers creates a single point of failure.
- **Inference Denial of Service:** A new breed of attack—flooding AI models with complex prompts to crash downstream agentic workflows—means that a CSP outage now freezes autonomous decision-making across entire industries.

Strategic Conclusion: The 2026 Operating Model

Success in 2026 will not be defined by perfectly predicting every regulatory outcome, but by building **governance capable of adapting to uncertainty**. Leaders should stop treating AI governance as a "documentation exercise" and start treating it as the core operating model for the intelligent age.

Three Concrete Actions for Leadership Teams:

1. **Adopt the "Three Lines of Defence":** Ensure the teams building AI (1st line) are overseen by an AI Ethics Review Board (2nd line), which is eventually audited by independent internal or external teams (3rd line).
2. **Implement Continuous Oversight:** Move away from "one-off" deployment approvals. Establish thresholds that trigger reviews when data drifts or when a model interacts with new systems.
3. **Prioritize Assurance Literacy:** Ensure your workforce understands not just how to **use** the tools, but how to **evaluate** their real-time actions and when to intervene.

The organizations that win in 2026 will be those that can prove their systems are **safe, secure, and beneficial**. In a landscape of "Supervised Reality," accountability is the fundamental prerequisite for deployment.

THE BOARD'S BLUEPRINT: 12 ACCOUNTABILITY QUESTIONS FOR AI GOVERNANCE

THE FOUNDATION: NIST AI RMF & EXECUTIVE OVERSIGHT

Adopt the NIST AI Risk Management Framework (AI RMF).

Align oversight with the core functions: Govern, Map, Measure, and Manage.

"AI RISK IS NOW FINANCIAL AND LEGAL RISK."

Governance must move from IT silos to the board level to prevent "governance debt."

GOVERNANCE AS AN OPERATING MODEL.

Shift from one-time deployment approvals to continuous monitoring and real-time guardralis.

12 QUESTIONS FOR BOARD ACCOUNTABILITY

1. MATERIALITY:
What high-stakes decisions is the AI influencing?

2. IMPACT:
Who can be harmed, and what are the societal consequences?

3. DATA PROVENANCE:
Where did data originate, and is there clear consent?

4. BIAS TESTING:
Has the system been tested for unfair demographic outcomes?

5. ROBUSTNESS:
Can the system withstand adversarial attacks or "tall events"?

6. EXPLAINABILITY:
Can we produce auditable documentation for every AI outcome?

7. HUMAN OVERRIDE:
Who is empowered to "kill" the system when it deviates?

8. SECURITY:
Are technical guardrails in piace to prevent model misuse?

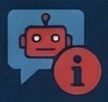
9. THIRD-PARTY RISK:
Do we have audit rights for our AI vendors?

10. MONITORING:
Is there a real-time dashboard for model drift and performance?

11. ACCOUNTABILITY (RACI):
Is there a "name on the hook" for every lifecycle stage?

12. DISCLOSURE:
Do users know they are interacting with an AI system?

11. ACCOUNTABILITY (RACI):
Is there a "name on the hook" for every lifecycle stage?



12. DISCLOSURE:
Do users know they are interacting with an AI system?

THREE LINES OF DEFENSE FOR AI GOVERNANCE

FIRST LINE
Model Owners/Quants: Continuous monitoring, drift alerts, and day-to-day remediation.

SECOND LINE
Risk & Compliance: Policy enforcement, setting fairness thresholds, and model validation.

THIRD LINE
Internal Audit: Independent assurance of the entire governance framework for the Board.

2026-03-03

It will get a little sporty in the Cloud Service Provider world in the days ahead!

Amazon Web Services (AWS) confirmed that two facilities in UAE (ME-Central-1) were struck by projectiles on Sunday March 1, 2026.

Fire started, power was cut. and of course outages. Enough said.

Then in Bahrain (ME-SOUTH-1) suffered impact from a projectile as well (not directly apparently). You can read more about that in the link below and there is a lot of reporting out there.

In one of our board meetings we talked about the importance of redundancy, and now this is playing out before us as we speak. This obviously continues to evolve as events unfold.

For financial institutions in Malaysia, the Bank Negara Malaysia "RMIT 2025" is starting to hit home but now it is not just about cyber-attacks, it is also for physical events such as what is happening in the Middle East.

Stand-In Processing becomes a critical component of the resilience engineering for key critical systems. It also raises concerns about the vulnerability of "Sovereign Cloud" hubs in geo political hotspots which is really the crux of the matter, the risk of relying on a single geographic region especially in a conflict zone, or even where your pipes would pass through an active conflict zone will be a concern.

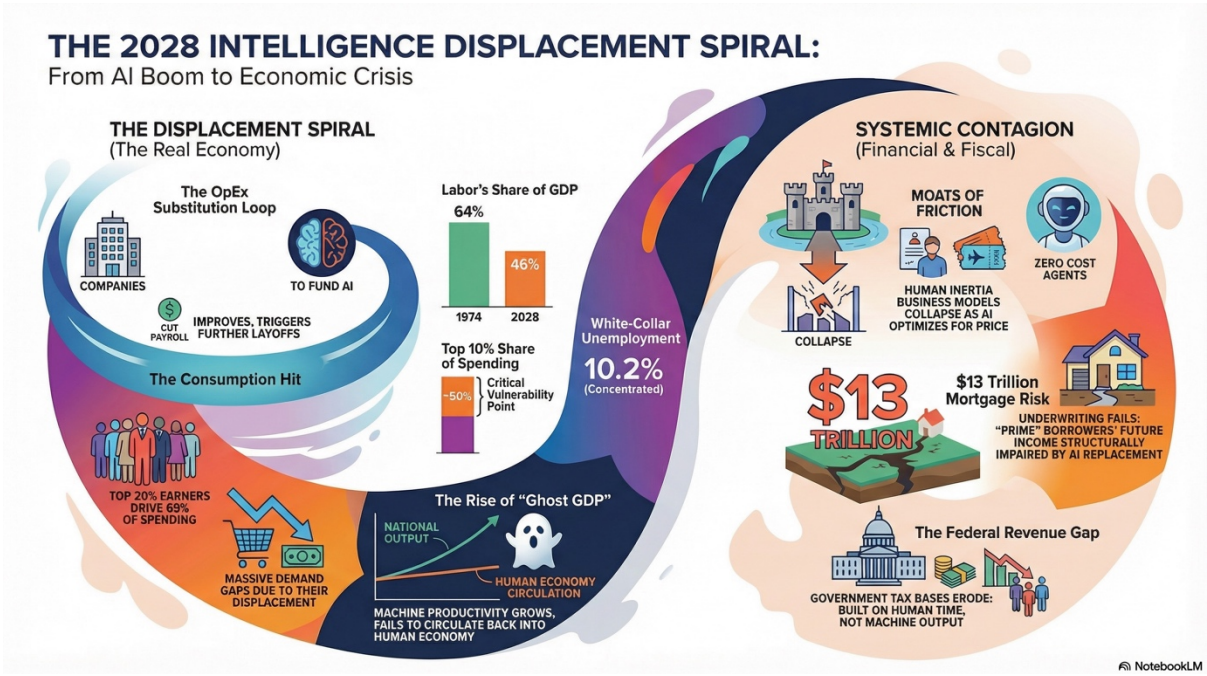
In the meantime, backup your data, and migrate critical workloads elsewhere as that operating environment is unpredictable.

hashtag#sovereigncloud hashtag#keycriticalsystems hashtag#rmit2025 hashtag#redundancy hashtag#backupdata

https://www.crn.com/news/cloud/2026/objects-strike-spark-fire-at-aws-data-center-in-the-middle-east

2026-02-24

The Paradox of Productivity: Navigating the "Ghost GDP" Scenario: What if the biggest risk with AI isn’t that it fails but that it succeeds too well, too fast?



A friend sent us a link to this article. It is a compelling macro thought experiment titled "The 2028 Global Intelligence Crisis." It moves past the technical "how-to" of AI and asks a much tougher question: What happens to a consumer-led economy when human labor is no longer its primary engine?

The scenario outlines a phenomenon called "Ghost GDP", a world where productivity and corporate margins soar because of AI, but that wealth stops circulating.

The logic is simple but startling:

Individual Rationality: A company replaces white-collar roles with agentic AI to stay competitive. It’s the right move for the balance sheet.

Collective Crisis: If every company does this, the high-earning "consumer class" loses its purchasing power.

The Loop: Machines are incredible at producing output, but they have a "marginal propensity to consume" of zero. They don’t buy homes, pay for insurance, or invest in retail.

The "Intermediation" Risk The piece suggests that any business model built on human friction, the complexity of navigating taxes, legal work, or financial products is at risk. When AI agents can handle these tasks with zero friction, the "value add" of entire service sectors could evaporate, creating a "race to the bottom" on pricing.

Navigating the Future For leaders and professionals, the takeaway isn't necessarily a "doomsday" forecast, but a call to broaden our lens. We are moving from a labor-centric economy to a capital/compute-centric one. This shift will test the resilience of everything from the mortgage market to private credit.

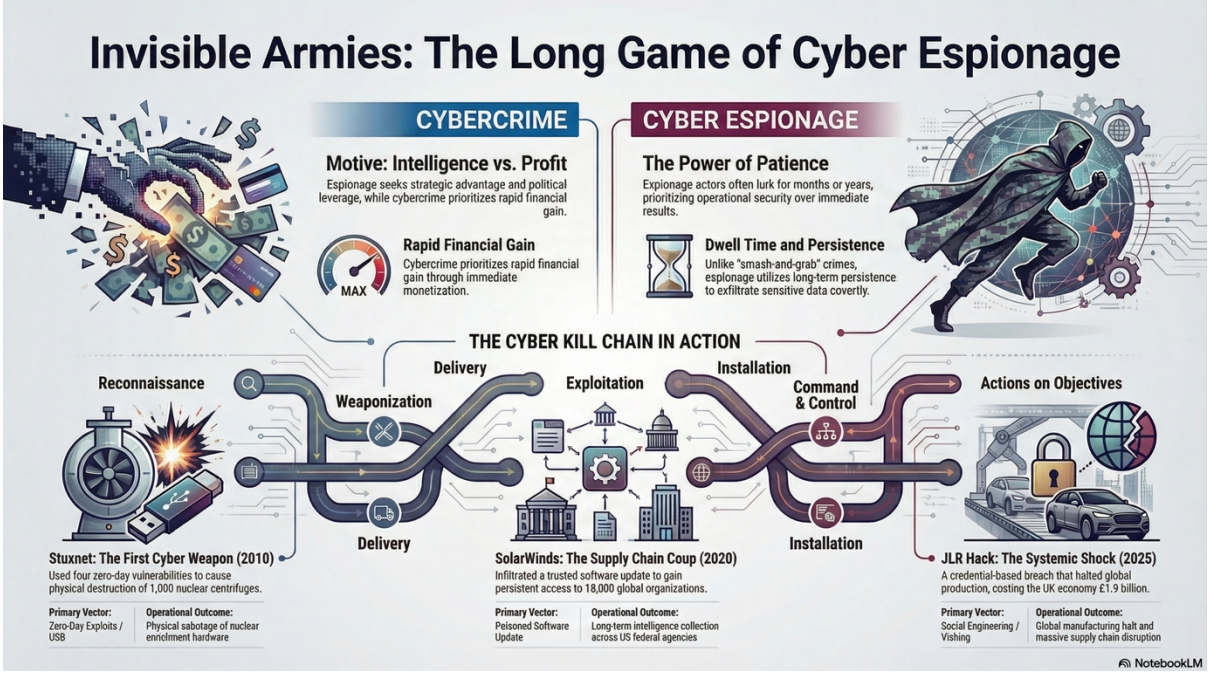
The challenge for the next three years isn't just adopting the tech, it's preparing for the structural shift in demand that follows.

How are you balancing the drive for AI efficiency with the long-term reality of a changing consumer base? Or do you think that this a credible scenario or too far off base?

hashtag#FutureOfWork hashtag#MacroEconomics hashtag#AI hashtag#StrategicLeader

2026–02–24

The Invisible War



Invisible armies are fighting a silent war where the ultimate weapon is information. While cybercrime targets immediate financial profit, cyber espionage focuses on long-term strategic intelligence gathering. Analysing high-profile case studies like Stuxnet, SolarWinds, and Jaguar Land Rover reveals how these competing motives reshape today's complex global digital landscape.

Click on the image to read the **article.**

Image with help of Notebooklm

Information and data points from a variety of different sources hashtag#cybercrime hashtag#cyberespionage hashtag#cyberkillchain hashtag#ciso hashtag#

Full Article

CISOs are going to have a busy 2026.

Invisible armies are fighting a **silent war** every second of the day, where the battlefield is not land or sea, but the digital networks that power our

modern world. In this "Invisible War," the ultimate weapon is **information**, and the motives behind the conflict determine whether we are witnessing a surgical act of **cyber espionage** or a high-stakes **cybercrime**.

Understanding the distinction between **intelligence gathering and financial profit** is critical for any leader navigating today's risk landscape.

Intelligence vs. Profit: Defining the Threat

The primary differentiator between these two digital threats lies in their **motive**.

Cyber Espionage is the act of using digital technology to gain unauthorized access to confidential or strategically significant information for the benefit of a nation-state, corporation, or organized group. It is traditional spying evolved for the digital realm. The goal is **decision advantage**: gaining insight for future negotiations, geopolitical positioning, or long-term economic competition. Key characteristics include:

- **Stealth and Persistence:** These are not "smash-and-grab" operations; they are designed to remain undetected for months or even years.
- **Strategic Targets:** Actors pursue military blueprints, trade secrets, diplomatic strategies, and critical infrastructure mapping.
- **State-Backed Resources:** Most cyber espionage is orchestrated by well-funded, patient, and highly skilled **Nation-State Advanced Persistent Threats (APTs)**.

Cybercrime, by contrast, is driven almost exclusively by **financial profit**. Whether through ransomware, credit card theft, or business email compromise, the intent is to convert digital access into cash as quickly as possible. While some organized criminal groups have adopted sophisticated "APT-style" tactics, their endgame remains the **ransom or the resale value** of data rather than strategic leverage.

Case Study 1: Stuxnet, The Strategic Saboteur

Discovered in 2010, **Stuxnet** remains the most famous example of a high-profile "cyber weapon". Unlike traditional malware designed to

steal data, Stuxnet was a computer worm created to cause **physical damage** to Iran's nuclear program.

- **The Operation:** It targeted Siemens Supervisory Control and Data Acquisition (SCADA) systems and Programmable Logic Controllers (PLCs) at the Natanz enrichment facility.
- **The Innovation:** Stuxnet utilized an unprecedented **four zero-day vulnerabilities** in Windows and was introduced via infected USB drives to hop across "air-gapped" networks.
- **The Impact:** By covertly altering the rotational speeds of gas centrifuges, it caused approximately 1,000 machines to physically degrade and destroy themselves while reporting "normal" readings to human operators.
- **The Lesson:** Stuxnet proved that cyber espionage could transition into **cyber warfare**, delivering kinetic results without a single missile being fired.

Case Study 2: SolarWinds, The Intelligence Coup

The 2020 **SolarWinds** attack (often referred to as **Sunburst**) redefined our understanding of **supply chain compromise**. Attributed to the Russian-backed group **APT29 (Cozy Bear)**, it was a masterclass in patient, widespread intelligence gathering.

- **The Method:** The adversaries infiltrated the build environment of SolarWinds, a trusted IT management vendor, and inserted a backdoor into a legitimate software update for their **Orion** platform.
- **The Scale:** Approximately **18,000 organizations** downloaded the tainted update, providing the attackers a "golden ticket" into the networks of the U.S. Treasury, the Department of Homeland Security, and hundreds of Fortune 500 companies.
- **The Cloud Shift:** What turned this from a breach into a crisis was the attackers' ability to move laterally into **cloud environments**. By abusing Microsoft identity and access management products, they pilfered email accounts and sensitive files silently for over nine months.
- **The Lesson:** Trust is now an **attack surface**. When the software you use to manage your network is compromised, your perimeter defense becomes irrelevant.

Case Study 3: Jaguar Land Rover, The Economic Siege

In September 2025, luxury automaker **Jaguar Land Rover (JLR)** became the victim of what has been called "the most financially damaging cyberattack in British history". Unlike the statecraft of Stuxnet or SolarWinds, this was an example of **organized cybercrime** at an industrial scale.

- **The Attack:** A group calling itself **"Scattered Lapsus$ Hunters"** likely used "vishing" (voice phishing) to trick employees into providing login credentials.
- **The Chaos:** The intruders moved from the IT network into JLR's **Operational Technology (OT)** network, the systems controlling physical assembly lines. To contain the threat, JLR was forced to **halt global production** for weeks.
- **The Impact:** The breach cost the company an estimated **£50 million per week** in lost revenue and caused **£1.9 billion** in damage to the wider UK economy due to the fragility of "just-in-time" supply chains. The attackers also exfiltrated **350GB of sensitive data**, including proprietary source code.
- **The Lesson:** Modern manufacturing is **"under siege"**. Outdated infrastructure and zero tolerance for downtime make manufacturers prime targets for **double extortion** (encryption plus data theft).

The Path Forward: Intelligence-Led Defense

The JLR attack and the SolarWinds coup illustrate that traditional defenses are failing against the most patient and well-resourced adversaries. For boards and executives, the "Invisible War" requires a shift from a compliance checklist to a **counterintelligence posture**.

1. **Shrink Dwell Time:** In espionage, the winner is determined by how long they can stay inside undetected. Organizations must prioritize **Mean Time to Detect (MTTD)** and **Mean Time to Contain (MTTC)**.
2. **Identity is the New Perimeter:** As seen in JLR and SolarWinds, compromised credentials are the "master key". **Zero Trust Architecture (ZTA)**, which eliminates trust based on network location is no longer optional; it is foundational.
3. **Harden the Supply Chain:** The use of **Software Bills of Materials (SBOMs)** must become standard to bring transparency to the thousands of third-party components integrated into

modern systems. The need for a continuous monitoring of vendor cybersecurity postures, with detailed **dependency mapping the Nth Party**.

4. **Operationalize Intelligence:** Threat intelligence is not a dashboard; it is a **decision advantage**. Leaders should constantly ask: "What did we do differently this quarter because of the intelligence we received?".

In this invisible war, the enemy is already inside the gates. The goal is no longer perfect prevention, but making espionage and crime **costly, noisy, and short-lived**. Stuxnet happened fifteen years ago, it is still worthy of a mention with all the lessons learnt from it.

The human operating system (**Human attack surface**) will remain our weakest link in the chain as Social Engineering methodology gets sophisticated with Gen AI, Deepfakes and everything that comes with it. **The need for a strong CISO is even more pronounced today than ever before.**

2026-02-20

Never assume reciprocity

A quote has been circulating:

“Expecting the world to treat you fairly because you are fair is like expecting a lion not to eat you because you didn’t eat the lion.”

It’s modern wording.
But the thinking behind it is old.

Niccolò Machiavelli warned rulers not to assume reciprocity.
Thomas Hobbes argued that without structure and power, life

becomes competitive and self-interested.
And centuries earlier, **Plautus** wrote: *“Lupus est homo homini”* — man is a wolf to man.

Different eras. Same observation.

Here is the uncomfortable governance truth:

Fairness is a personal value.
It is not a market mechanism.
It is not a regulatory safeguard.
It is not a defence strategy.

In boardrooms, I have seen this mistake repeatedly:

Good people assume that because they are transparent, others will be transparent.
Because they are principled, others will act in good faith.
Because they disclose risk, others will reciprocate.

That is not how power works.

The world operates on incentives.
It operates on leverage.
It operates on consequence.

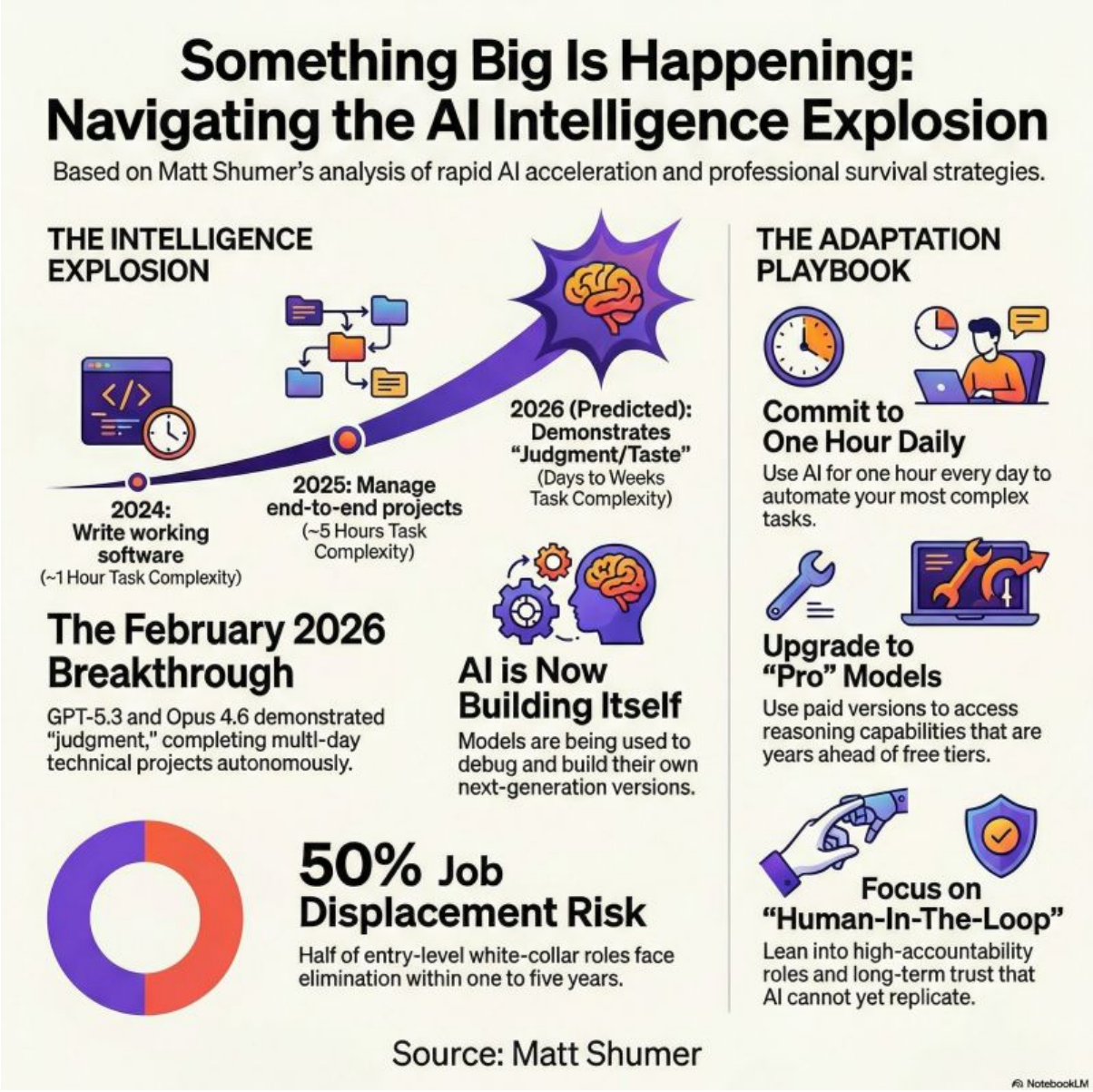
You must remain fair.
But you must not be naïve.

Strong governance is not cynicism.
It is clarity.

Be ethical.
Be principled.
But understand the lion.

2026-02-22

Something Big Is Happening and Most People Are Still Asleep



I just read a striking essay by Matt Shumer, titled “Something Big Is Happening” (published on shumer.dev), and I think it deserves the attention of every board member, CEO, professional and just about anybody out there who still believes AI is “just another tech trend.”

Shumer's core message is blunt: the AI shift is not coming, it is already here. And it will be more disruptive than most people are prepared for.

What makes his argument uncomfortable is not hype, but timing. He points out that the pace of capability improvement in modern AI systems is no longer linear , it is compounding. Models released today are dramatically more powerful than those from even six months ago. This is not about chatbots writing emails.

Shumer argues we are entering an era where AI systems demonstrate something closer to judgment , not merely following instructions, but making decisions, solving problems, and increasingly performing the kinds of cognitive work that define white-collar employment.

His warning is direct:
If your job involves reading, writing, analysing, reporting, planning, or managing information on a computer, AI will touch it , sooner than expected.
And unlike past waves of automation, this is not limited to one narrow function at a time. AI is becoming a general substitute for a wide range of mental labour. Entry-level roles in law, consulting, finance, compliance, and administration are especially exposed.

Shumer also highlights a deeper acceleration: AI is starting to help build the next generation of AI, compressing innovation cycles even further. OpenAI confirmed GPT-5.3 Codex was instrumental in creating itself debugging its own training and managing deployment.

His conclusion is not panic but it is preparation.

The practical call is simple: Stop treating AI as a curiosity. Start treating it as infrastructure. And move to the paid versions….

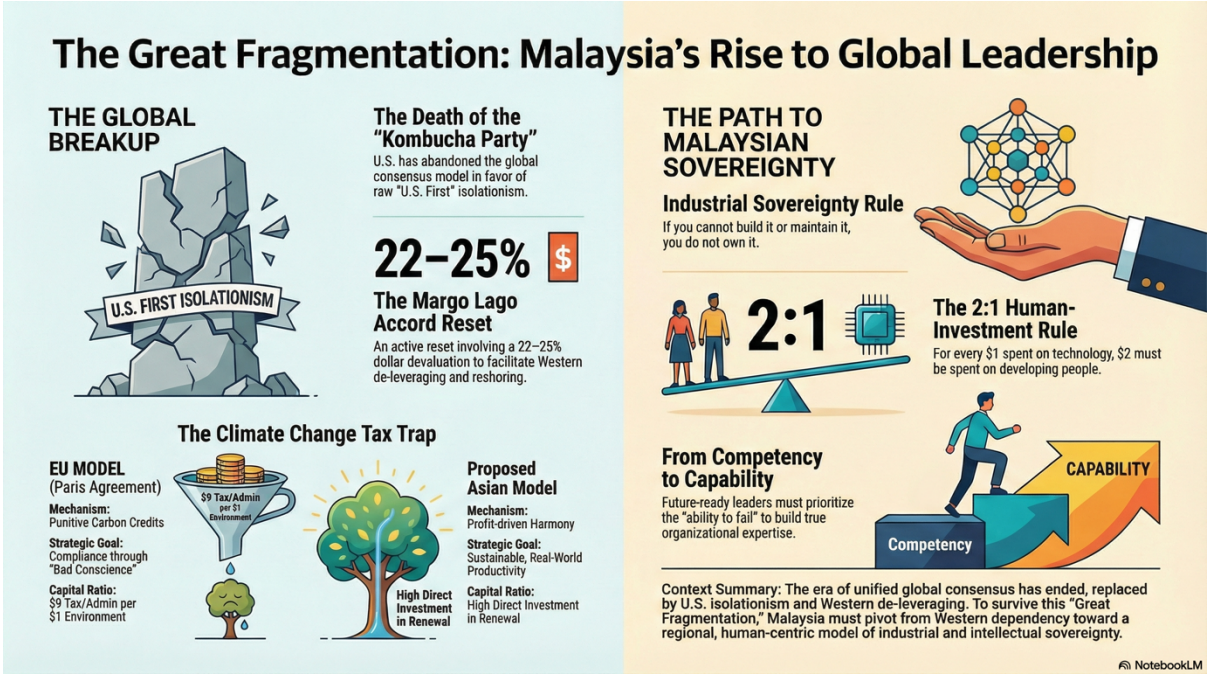
Those who integrate these tools early will gain leverage. Those who dismiss it as "overhyped" may find themselves reacting too late, using yesterday's assumptions to explain tomorrow's reality.

As Matt Shumer writes: something big is happening. The question is whether leadership is paying attention.

I used Notebooklm to produce the infographic.

2026-02-08

The "Kombucha Party" is Over: Navigating the Great Fragmentation



An Extract from Professor Henrik von Scheel's talk on Feb 5 2026.

The global consensus hasn't just slowed down; it has experienced a definitive "breakup". For decades, the global economy operated as a "Kombucha party"—a U.S.-led model where nations held hands. That era is dead. We are witnessing "U.S. First" isolationism, a calculated abandonment of the house the U.S. built because globalization no longer serves their secured market.

The Mar-a- Lago Accord: A Radical Reset This isn't hypothetical; it's an active reset of the global monetary system. Triggered by the "divorce" between the petrodollar and Saudi Arabia, the U.S. is de-leveraging through five pillars:

1. Targeted dollar devaluation (22–25%),
2. Manufacturing reshoring,
3. Aggressive tariffs,
4. Capital repatriation,
5. and Resource capture.

The "Climate Change Wars" Malaysia must stop "drinking the European Kool-Aid". The current EU model is a failure, where $9 out of every $10 spent goes toward administration rather than the environment. This is a tool of control designed to impose "bad consciousness" on Asia. Instead, Malaysia should lead with Regional Circularity and Harmony.

Industrial and Intellectual Sovereignty In this new era, manufacturing is the "hardcore backbone". But there is a golden rule: If you cannot build it or maintain it, you do not own it. We must move beyond being a mere assembly point and build our own robotics to avoid technological colonization.

Regarding AI, 35–45% of investments are expected to evaporate. We must guard against "Shadow AI" and the "Innovation Theatre" that exports proprietary data to foreign LLMs. Follow the 2:1 Investment Rule: for every $1 spent on technology, $2 must be spent on people.

Islamic Finance & the Real Economy As a leader in Islamic Banking, Malaysia can "unweaponize" capital. Islamic Finance must act as the "loyal enforcer" for the Real Economy, linking directly to tangible trade and manufacturing rather than speculative fluctuations.

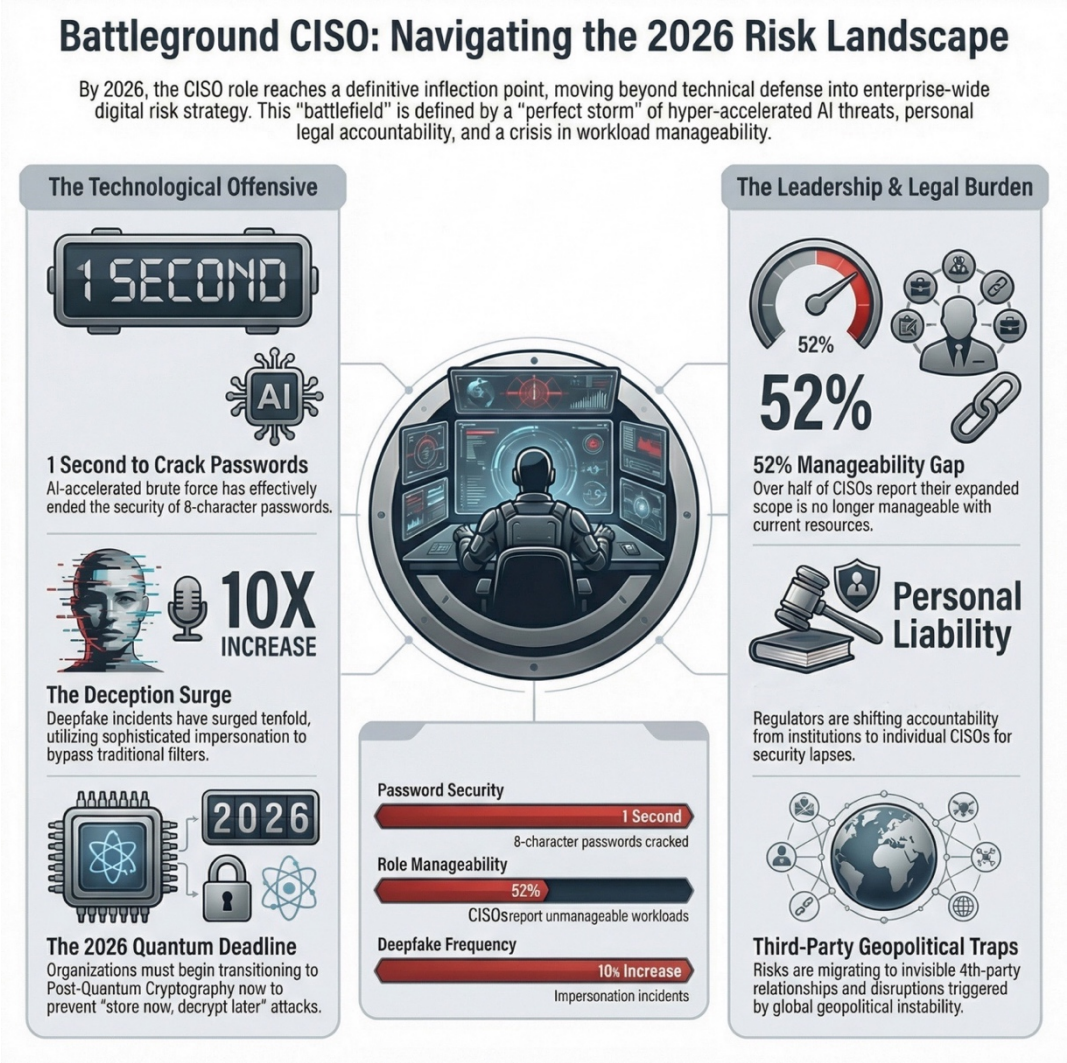
Malaysia: The "Carrier of Hope" The tectonic plates are shifting East. While the West is disillusioned, the youth of Asia still believe in the future. To lead, we must focus on Capabilities—the ability to build expertise through failure—rather than static competencies.

The torch of leadership is in our hands. By focusing on human-centric innovation and ethical finance, Malaysia will lead a wealthier world. The future is human. The time to lead is now.

hashtag#Geopolitics hashtag#Malaysia hashtag#IndustrialSovereignty hashtag#

2026-02-23

Navigating the 2026 Executive Cybersecurity Outlook



1. The Great Strategic Shift: From IT Function to Growth Catalyst Cybersecurity has evolved from a back-office IT function to a top-tier business risk and growth catalyst. We must transition from "technical framing" to "strategic impact" to thrive. Cyber resilience is the "So What?" factor for innovation, enabling three core growth opportunities:
* Revenue potential (71%)
* Ecosystem development (68%)
* Geographic expansion (56%)

Resilience is a competitive advantage in a world of geopolitical flux. This mindset is vital as we navigate the dual-edged nature of AI.

2. The AI Paradox: Managing the Sword and the Shield AI is a "Dual-Use" technology. It powers defence but has doubled malware samples since 2016 via "WormGPT" and FraudGPT automation.
The Sword: Deepfakes have sparked a "Crisis of Identity." A $25M Hong Kong loss via a cloned CFO proves that Deepfake Drills and verification protocols are now mandatory. The Shield: We must move to AI-led predictive modelling and prioritize controls that reduce exposure from Shadow AI.
As AI weaponizes identity, the "Regulatory Vice" is tightening around personal leadership.

3. The Regulatory Vice and Structural Leadership Evolution pressure and a "Trust Deficit" demand Board-level engagement. Incidents must be disclosed within four business days, and regulators are now pursuing personal and criminal liability. Bank Negara Malaysia issued the latest Policy Document, RMiT 2025.

To escape the "Watermelon Reporting Trap" (Green compliance masking Red risk), 47% of CISOs now hold SVP/EVP titles, while 36% report to business leaders (CEO/GC) to ensure independence.
Shift to Business-Centric Metrics:
* Revenue at Risk (Quantified exposure)
* Vendor Ecosystem Risk
* Assurance (Evidence of containment)
This shift moves focus from current compliance to a forward-looking roadmap.

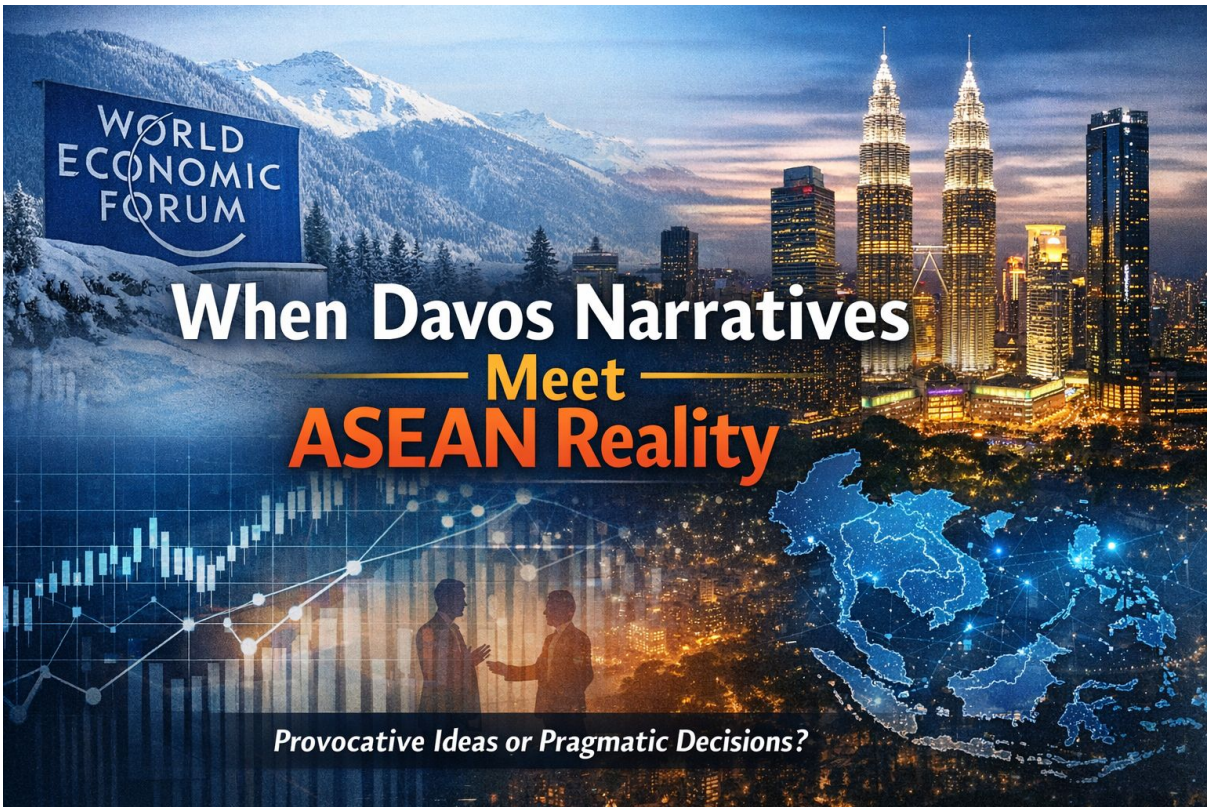
4. The 2026-2027+ Strategic Roadmap We must embrace Crypto-Agility to counter the "Quantum Horizon" (Harvest Now, Decrypt Later).
* Now: Modernize infrastructure and review vendor contracts for SEC alignment.
* Near-Term: Deploy Responsible AI and address CISO burnout (52%). Burnout compromises decision-making during incidents.
* Long-Term: Execute Post-Quantum migration and leverage Digital Trust as a sales differentiator.

Executive Mandate: "The firms that pull ahead will be those that make cybersecurity a board-led capital decision." — PwC

Slide Deck produced using Notebooklm

2026-02-05

When Davos Narratives Meet ASEAN Reality



Today I listened to Professor Henrik Von Scheel speak on “Unlocking the Future of Finance in Asia.”, a high profile Davos linked futurist and pioneer of the Fourth Industrial Revolution at the AICB Centre of Excellence (Feb 5, 2026) organised by the Asian Banking School, and Strategic Intelligence World Economic Forum.

He is a compelling voice, the kind of futurist who speaks in tectonic shifts:
de-globalisation, AI disruption, industrial resurgence, the eastward movement of economic power. The need to go down the path of manufacturing nationalism.

I didn’t agree with every conclusion.

But I left with a useful reminder: Keynotes provoke. Boardrooms must

decide.

The challenge for financial leaders in Asia is not whether we embrace every global narrative but whether we ask the right questions beneath them:

Are we treating AI as strategy… or as uncontrolled data leakage? Or is it a real systemic risk? and will the hype blow over?

Is “industrial policy” a slogan, or a serious competitiveness plan?

How resilient is our financial system if geopolitics fragments markets further? Financial resilience is tied to real economy assets.

And most importantly: can Asia shape its own path without importing someone else’s template? Will we be allowed to?

The future of finance in this region will not be built on hype but on disciplined governance, real assets, and institutional trust.

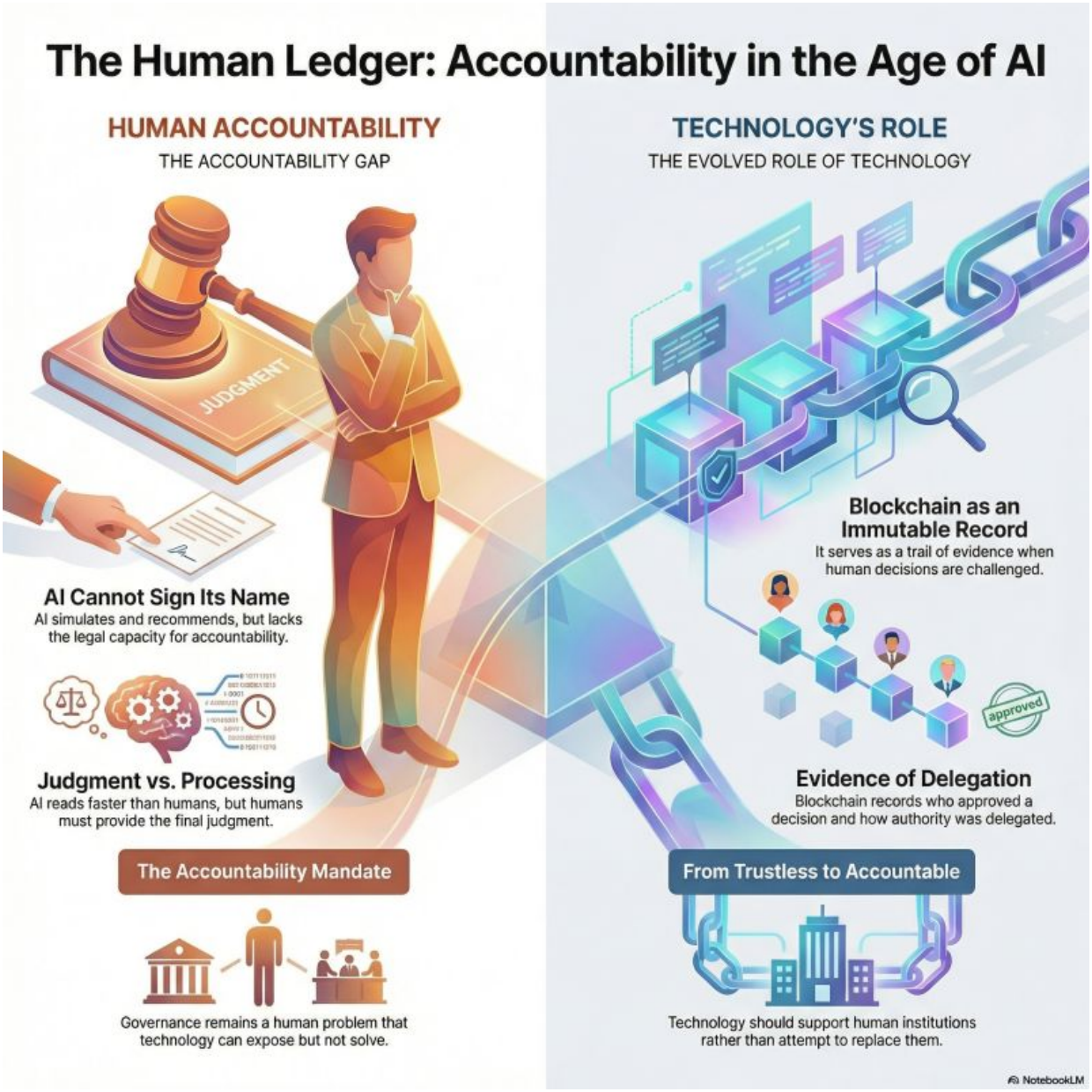
Curious: what is the most overrated trend in finance right now and what is the most underestimated?

If you get a chance, have a listen, he does make a good case and is provocative as well. I enjoyed the session.

hashtag#professorhenrikvonscheel hashtag#highvoltagespeaker hashtag#tectonicshifts hashtag#asiaisnotajuniorpartner

2026-02-01

HUMANS IN THE LOOP



For nearly a decade, blockchain promised something radical:
a world that didn't need trust. Then GenAI arrived.
Large language models didn't make governance "trust less" but they made it judgement-heavy again. That's the uncomfortable truth many haven't absorbed yet:

Blockchain is excellent at one thing: making history hard to rewrite.
AI is excellent at another: interpreting messy reality and proposing action, with all the hallucinations and bias built-in.

The mistake is thinking they compete. In board governance, land registries, supply chains, and now AI agents acting on behalf of directors, the real battleground isn’t technology it’s accountability.

AI will digest mountains of information, surface risks and inconsistencies and propose options and trade-offs. But be careful, it cannot be the accountable party, that role still sits with humans (us directors).

Blockchain, if used at all, belongs below the decision layer — as a notary, not a brain. Recording what was authorised, by whom, and when.

AI makes thinking cheaper.

Blockchain makes history harder to rewrite.

Humans remain responsible.

Boards that don’t internalise this will either over-delegate to AI or chase the next hype cycle. Neither ends well.

2026-01-26

Character, Unity, and the Scourge of Corruption

In his 2026 royal address, His Royal Highness the Yang di-Pertuan Besar of Negeri Sembilan emphasises the critical need to balance academic success with moral development. The Yang di-Pertuan Besar expresses grave concern over rising social ills among youth and advocates for early childhood education modules that instil noble values and discipline.

Beyond the classroom, he highlights community involvement and mutual respect as essential tools for building a unified, ethical society.

A significant portion of the speech is dedicated to a stern condemnation of corruption, which he identifies as a destructive force against national integrity and justice.

Ultimately, the address serves as a call for collective responsibility to reform the character of future leaders and reject criminal behaviour at all levels of society.
hashtag#yangdipertuanbesar hashtag#royaladdress hashtag#daulattuanku

Building a Future of Character and Integrity

SHAPING FUTURE GENERATIONS THROUGH EDUCATION

Education Beyond Academic Success

Academic achievement must be paired with strong character and moral values to prevent social ills.

The Aulad Sejahtera Module

A foundation for preschoolers to learn respect, environmental care, and mutual cooperation.

Holistic Secondary Development

Participation in uniformed bodies and clubs builds **discipline, leadership,** and a spirit of **volunteerism**.

THE FIGHT FOR INTEGRITY AND TOGETHERNESS

The Spirit of Togetherness

A willingness to understand and respect others across different races, religions, and backgrounds.

Zero Tolerance for Corruption

Corruption is the principal enemy of justice and erodes the moral foundations of society.

"Any compromise is unacceptable"

Citizens must introspect and stop supporting individuals convicted of serious corruption offenses.

Excerpt from the Royal Address

His Royal Highness The Yang di-Pertuan Besar of Negeri Sembilan Darul Khusus

(Paragraphs 7 to 14)

In Conjunction with the 78th Birthday Celebration of

His Royal Highness the Yang di-Pertuan Besar of Negeri Sembilan Darul Khusus

Wednesday, 14 January 2026 Istana Besar Seri Menanti

10. At the secondary education level, students should be encouraged to actively participate in school societies and clubs as a platform for building identity, character, and leadership. Participation in uniformed bodies as well as clubs centred on sports, welfare, and the spirit of *gotong-royong* (mutual cooperation) is not only able to instil discipline and a sense of social responsibility, but also strengthens values of care, cooperation, and volunteerism, all of which are essential in shaping a generation that is ethical, credible, and well-balanced.

11. I have frequently highlighted the importance of the spirit of togetherness in my recent addresses. This spirit of togetherness refers to the willingness of the people to understand, respect, and cooperate with one another across differences of race, religion, and background. Undoubtedly, every race and religion has its own values and culture. I am confident that a holistic and continuous educational approach, grounded in the implementation of the *Aulad Sejahtera* Module as a foundation for value formation, will produce a future generation endowed with a strong spirit of togetherness. This spirit is of great importance and should be instilled and embraced by all members of society as an integral part of the principles of communal life.

12. Therefore, in the effort to shape future society, education must begin from early childhood. As stated by the Prophet Muhammad (peace be upon him):

“There is no gift that a father can give to his child more virtuous than good education.”

(Hadith narrated by al-Tirmidhi)

I wish to stress that this exhortation is directed at all levels of society, in both rural and urban areas, across all races and religions. Hence, all parties must work hand in hand in educating and guiding the younger generation as the leaders of the future. This collective effort is crucial in ensuring a more glorious future for the state and the nation.

The Scourge of Corruption

13. At the same time, I firmly state my position on the scourge of corruption, which appears to be increasingly rampant and deeply alarming. Corruption is the principal enemy of justice, trust, and the future of the nation. I am greatly shocked and disappointed that there are still parties who continue to support individuals who have been convicted of serious corruption offences, as though such actions are acceptable and forgivable. Such attitudes not only reflect a failure to understand the dangers of corruption, which not only erodes institutional integrity and the moral foundations of society, but also demand a deeper reassessment of one's faith, principles of life, and core values.

14. In this regard, I call upon those who continue to support such criminals to immediately engage in introspection and reassess their stance and beliefs. This is because any form of tolerance or compromise towards corruption is contrary to the principles of truth, justice, and trust, and is wholly unacceptable in a country that upholds the rule of law.

7. The educational performance of Negeri Sembilan has shown an encouraging upward trend. This achievement reflects the continuous commitment of all parties and should be further strengthened. Nevertheless, success in the academic field must go hand in hand with the development of strong character and moral values.

Early Education Shapes the Future Generation

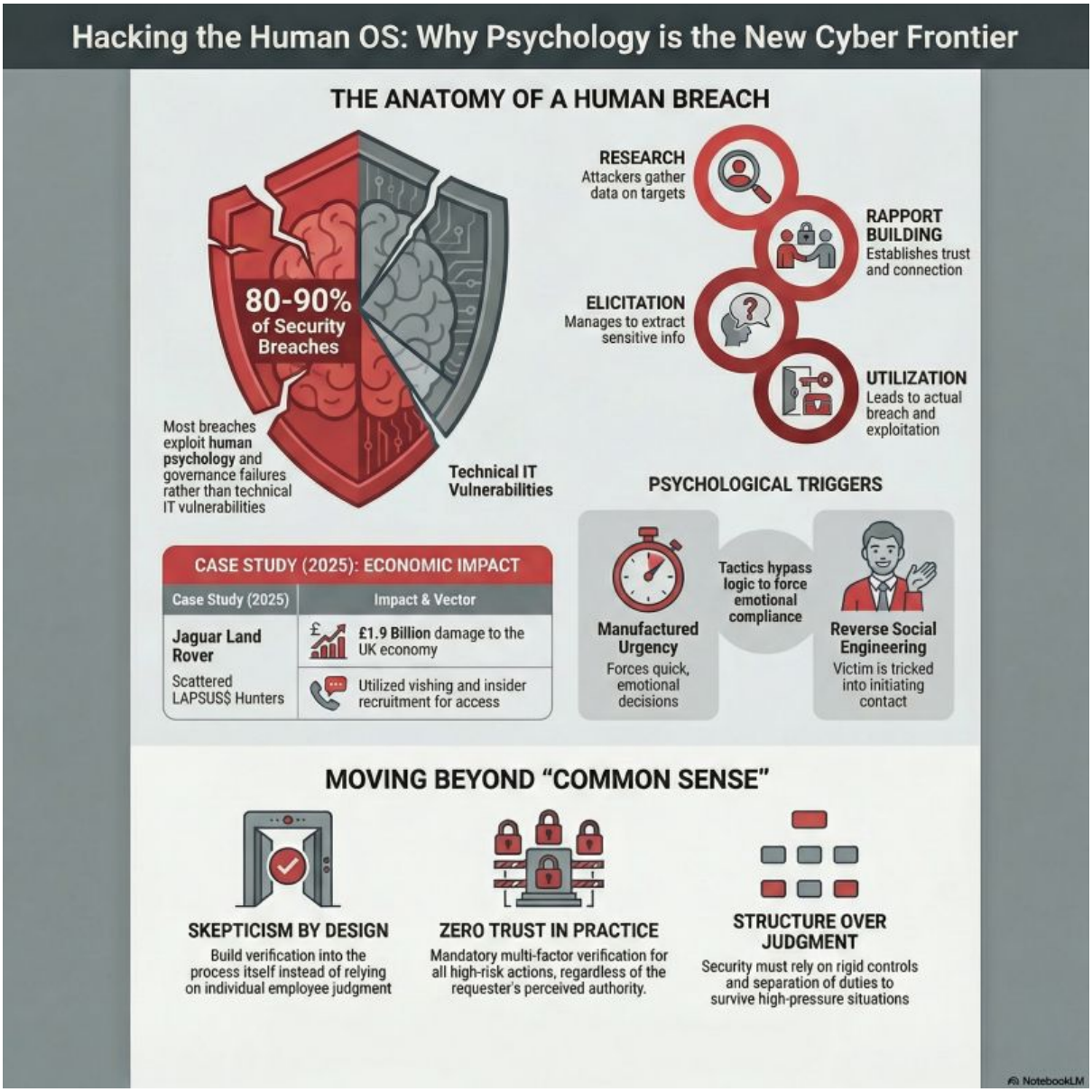
8. I am deeply concerned about the increasingly worrying social ills among today's younger generation, including drug abuse, illegal motorcycle racing, and various negative behaviours that can jeopardise their future. These problems not only have adverse effects on individuals, but also undermine family harmony and the overall well-being of society.

9. I have previously emphasised that education is the most fundamental foundation in shaping the character and identity of children from the earliest age. I therefore welcome the initiative of the Negeri Sembilan Islamic Religious Council (MAINS) in implementing the *Aulad Sejahtera* Module at the preschool level over the past two 2

years. This module places strong emphasis on the inculcation of noble values such as respect for parents and elders, love and care for the environment, a spirit of helping one another, and cooperation. I hope that this highly relevant module will be continued and its implementation expanded to the primary school level, to ensure continuity in the development of good character among children. This will also ensure that the noble values instilled through this module are reinforced on an ongoing basis, and ultimately remain as guiding principles that shape their character into adulthood.

2026-01-10

HACKING THE HUMAN OPERATING SYSTEM – SOCIAL ENGINEERING



In the previous post I eluded to the idea that we should start moving to building a “No-Blame” culture for the people, in this piece, I advocate “Zero Trust and "scepticism by design", in a complete reverse of trying to build trust.

80% to 90% of all security breaches share one common factor: they

don’t exploit code; they exploit the “human operating system”.

In the world of cybersecurity, social engineering is a human governance failure vector, not a purely technical IT problem,. It relies on the manipulation of universal psychological traits that are inherent in all of us regardless of our intelligence or professional experience.

Why are these attacks so effective? Attackers use a structured four-stage cycle that being Research, Rapport Building, Elicitation, and Utilization grounded in timeless psychological principles:

Authority & Obedience: Authoritative experiments, such as the Milgram study, demonstrate that 65% of individuals will obey an authority figure even when it contradicts their own judgment.

Reverse Social Engineering: A cunning social engineer may actually create a problem and then position themselves as the solution, allowing the victim to approach the attacker voluntarily.

Orchestration of the “Own Idea” approach. Attackers manage the target’s ego by listening more than they speak and confirming the target's opinions. By subtly guiding the conversation, the social engineer leads the target into believing that the final solution or action was actually their own idea.

The Power of Reciprocity: Humans feel an unearned sense of obligation to return favours, a trait attackers exploit by giving "small gifts" or "help" before making a sensitive request.

Urgency (Pathos): By manufacturing a crisis or a strict deadline, attackers bypass our rational logic (Logos) to force a rushed, emotional decision.

We saw this play out at a massive scale in the Jaguar Land Rover (2025) case,
where the Scattered LAPSUS$ Hunters alliance utilized vishing and insider recruitment to cause an estimated £1.9 billion in damage to the UK economy, three weeks of total production shut down and not to mention that this digital siege brought a giant to its knees.

The Takeaway for Leaders: Intelligence is not a shield,. To protect our

organizations, we must move away from relying on employee "common sense" and instead implement: ✅ Scepticism by Design: Building verification into the process itself,. ✅ Zero Trust in Practice: Mandatory multi-factor verification for all high-risk actions, regardless of who is asking,. ✅ Structure over Judgment: Security must be based on rigid controls and separation of duties, as personal judgment often collapses under authority and pressure.

In a world of sophisticated human-centric threats, trust without accompanying controls is a form of negligence.

Dangerous times.

hashtag#CyberSecurity hashtag#SocialEngineering hashtag#Governan

2026-01-05

Are We Just Managing Yesterday's Risks?

The line between "traditional" crime and cybercrime has officially vanished (blurred). If you are still viewing cyber threats as a niche IT issue, you are missing the economic and social layer where the most significant damage now occurs.

We need to stop looking at "technical theatrics" and start addressing cyber-enabled crimes, traditional offenses like fraud and harassment,

are now accelerated by Generative AI to achieve unprecedented scale.

The New Reality for Leaders:

· Gen AI is the Amplifier. Most real-world damage today stems from fraud, not just "hacking." Generative AI has lowered the barrier to entry, allowing criminals to craft unspottable phishing and deepfakes at zero marginal cost.
· The "Global Franchise" vs. Your Supply Chain. We aren't fighting lone hackers; we are up against a Crime-as-a-Service (CaaS) economy. Meanwhile, our biggest risks often sit with our vendors. If you aren't watching your third parties, you've left the back door open.
· The Governance Grey Zone. Many failures occur because a risk is "known" but lacks accountability. This is especially true for online harms dismissed as "HR problems" rather than core security risks.

Moving Beyond "Tick-Box" Compliance

Having an ISO 27001 certificate is a start, but policy compliance is not the same as protection. Real resilience requires:

1. Quantifying Risk in Financial Terms. Maybe we should stop showing the Board "Red/Amber/Green" heatmaps. Start discussing Probable Maximum Loss and EBITDA impact.
2. Building a "No-Blame" Culture. Phishing isn't just a technical glitch; it's a human process failure. If your employees are too scared to report a mistake instantly, you lose the most critical factor in recovery: Time.
3. Focusing on Tail Risk. Prepare for the extreme outliers rather than relying on misleading industry averages.

The Bottom Line: Cyber risk is less about prediction and more about preparedness. Boards fail when they don't insist that controls work where it hurts the most.

Three questions every Chair should ask today:

1. The Financials: If our primary payment or operational system goes down for 48 hours, what is the exact financial impact?
2. The Supply Chain: We know our own recovery time, but do we know the recovery time of our three most critical vendors?
3. The Human Element: Where exactly can money move without a

human challenge—and how are we validating identity in an age of deepfakes?

hashtag#CyberSecurity hashtag#RiskManagement hashtag#Governa