



»»» SOUTHEAST ASIA TECHNOLOGY TRENDS & PRIORITIES FOR 2024



Contents

Segment 1:

Board & CEO Priorities for the New Technology Landscape

Segment 2:

Building Readiness & Agility in Enterprise A.I.

Segment 3:

Fostering Data Trust, Strengthening Data Ownership & Defending Data Privacy

Segment 4:

Building a Sustainability-Conscious Technology Organisation

ABOUT SPARK

SPARK (formerly CIO Academy Asia) helps leaders succeed in a fast-changing world driven by technology advancements. We create platforms where CIOs, business leaders and thought leaders share their insights, knowledge and expertise with the wider community of executives in business, government and technology community organisations. We help our community of C-level leaders to stay ahead of the industry by navigating the evolving technology landscape with new and practical knowledge shared by their peers.

For more information, visit <https://wahspark.com/>

Segment 1:

Board & CEO Priorities for the New Technology Landscape

In 2024, boards of companies and their leaders are prioritizing a diverse range of initiatives to navigate the rapid pace of technological change and respond to game-changing macro-shifts economic and geo-political shifts, as well as technology disruption all at once. These priorities reflect a strategic focus on sustainability, digital transformation, fostering data trust and building stakeholder confidence, which all converge into a singular theme: building agile, learning organisations to keep pace with today's rate of change and uncertainty.

1a. A.I.'s Influence on Board Leadership Priorities

2 in 3 

Recent developments in A.I. are reshaping board leadership priorities by emphasising the need for agility and resilience in organisational structures. A.I. technologies, particularly generative A.I., are driving the surge in curiosity in experimentation across various business functions, from customer service to product development.

Board members are adequately equipped to make informed decisions about A.I. opportunities & navigate potential challenges.

Boards must ensure that their organizations are not only prepared to integrate these technologies but also capable of doing so in a way that promotes innovation and responsible experimentation. This means establishing governance frameworks that address A.I. risks, such as ethical considerations and data privacy, while also fostering an environment where A.I. can be used to enhance decision-making and operational efficiency.

A note of optimism can be found at the top among board leaders in Asia, with 63% of boards showing to possess an adequate level of understanding of A.I. and its potential applications, with another 14% of board leaders showing a higher degree of preparedness and are actively engaged to deepen understanding in the impact of A.I. across the organisation.

Boards play a central role in shaping the strategic direction of an organization. An in-depth understanding of A.I. ensures that strategic decisions align with the transformative potential of A.I. technologies. As A.I. implementation introduces technological and ethical challenges that require informed decision-making, such developments will require the deep expertise of boards, especially in risk management, audit and technology

committees, to be applied into unfamiliar territories defined by new A.I. innovations. Informed boards contribute to optimal resource allocation, directing resources towards A.I. initiatives that align with the organization's overall objectives, fostering innovation and competitiveness. Most importantly, stakeholder confidence is bolstered when boards exhibit awareness and proficiency in A.I., meeting the growing expectations of investors and customers in navigating the evolving technological landscape.

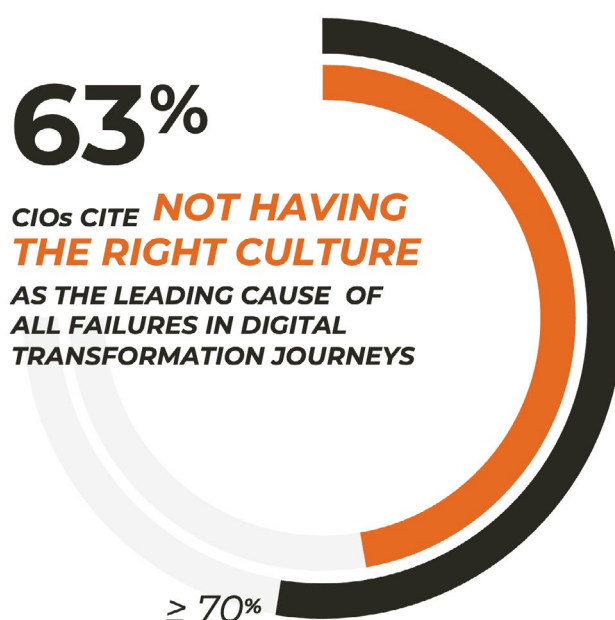
1b. Rethinking Board Composition Suitable for Building Effective Learning Organisations

Board compositions in Asia, particularly in Southeast Asia and Singapore, have traditionally been less diverse compared to those in the US and Europe. However, there has been a growing trend towards diversification, including gender, age, and professional background, as companies recognize the value of diverse perspectives in driving innovation and navigating complex global markets.

With more technology leaders being appointed to boards to guide digital transformation initiatives and ensure that companies are well-positioned to leverage emerging technologies such as AI, big data, and the Internet of Things (IoT), while augmenting deep expertise on technology governance and digital transformation roadmaps. The National Association of Corporate Directors (NACD) data shows that the growth rate of technical board additions has held steady over the past three years. In 2020, 43% of board directors at S&P 500 companies and 38% of those in Russell 3000 companies had technology backgrounds mentioned in their bios, up from 34% and 33%, respectively, in 2018.

1c. Learning is the Only Way Forward, Going Beyond Classical Change Management Strategies

Boards must build learning organisations to maintain agility during times of rapid disruption and uncertainty because such organizations are better equipped to adapt to change. Today's change management are often ad-hoc, with outcomes struggling to leave a sustained impact. A learning organisation is one that actively cultivates the growth and development of its members, fostering a culture of continuous improvement and innovation. This approach is crucial in today's fast-paced business environment, where the ability to learn and apply new knowledge quickly can provide a competitive edge. Learning organizations are characterized by their ability to challenge the status quo, embrace new ideas, and leverage collective knowledge to navigate complex problems.



Segment 2:

Building Readiness & Agility in Enterprise A.I.

Survey Question:

How well-prepared do you think your organisation is to adapt to the evolving global A.I. landscape?

Very Well-Prepared

Strategy is agile and responsive to emerging challenger

9%

Well-Prepared

While there's readiness, improvements can be made

53%

Neutral

Preparedness hasn't been a major focus but is worth considering

29%

Not Well-Prepared

There's a need to enhance our overall readiness

9%

2a. Organisational Readiness

Global race to put A.I. in the hands of consumers, “Free-to-Try” spurs awareness and experimentation, effective in building organisational readiness.

The survey of C-suite leaders from both private and public sector organisations provides valuable insights into the perceived preparedness of tech leaders on the C-suite for the evolving global A.I. landscape.

Notably, a majority, constituting 62% of the respondents, exhibit a positive outlook. Among them, 9% assert that their organisations are very well-prepared, citing an agile strategy that remains responsive to emerging challenges. Additionally, 53% express a level of preparedness but acknowledge room for improvement within their current strategies.

While A.I. isn't new to organisations, new capabilities that provide further democratisation of A.I., such as low-code or no-code, natural language processing

(NLP) and multi-modal generative A.I. technologies, provide a great deal of education and awareness to organisations, beyond the traditional walls of the I.T. team.

Bridging the knowledge gap has always been a challenge for organisations to bring its workforce into the A.I. age. In this new “free-to-try” age, the novelty of recent breakthroughs and global hype of generative A.I. features, have prompted the average consumer to get hands-on with A.I. and think creatively about how such technologies could be applied to their work. Gartner's recent survey provide compelling evidence, with 55% of organisations that have previously deployed A.I. always consider A.I. for every new use case that they are evaluating.

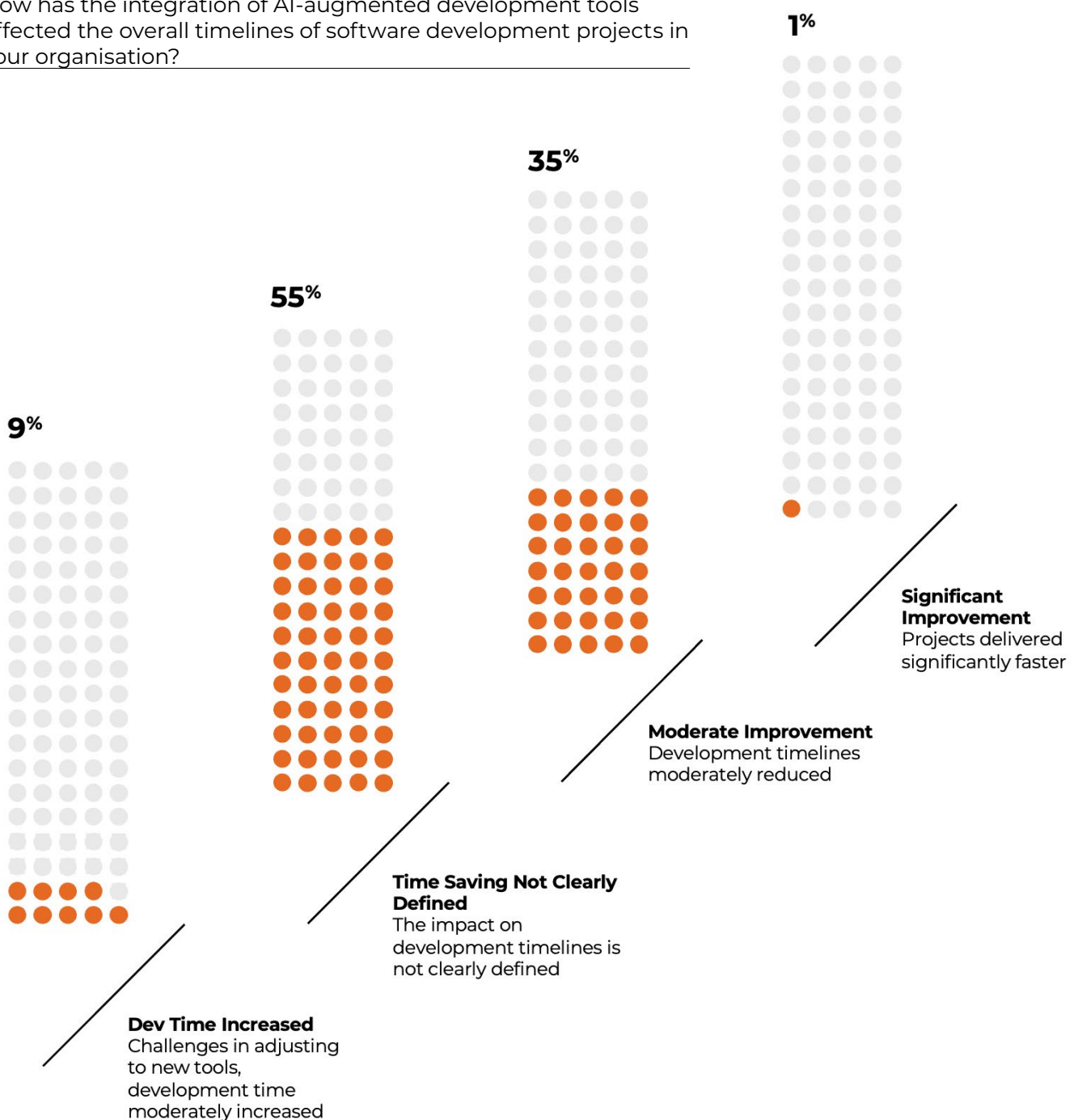
While a majority of C-suite leaders demonstrate confidence in their organization's A.I. preparedness, the nuanced responses mirror the complexity of A.I. adoption. The findings underscore the importance of addressing skill gaps, integrating A.I. seamlessly, and establishing robust ethical frameworks for sustained success in navigating the evolving global A.I. landscape.

2b. A.I. Co-Pilots will mature through the Adoption Curve

The potential of AI co-pilots in the digital transformation journey is substantial. AI-augmented tools can automate routine tasks, enhance code quality, and provide insights that lead to more innovative solutions. However, the survey data highlights the importance of addressing compatibility with legacy systems and ensuring that organizations are culturally and operationally prepared to embrace these technologies.

Survey Question:

How has the integration of AI-augmented development tools affected the overall timelines of software development projects in your organisation?

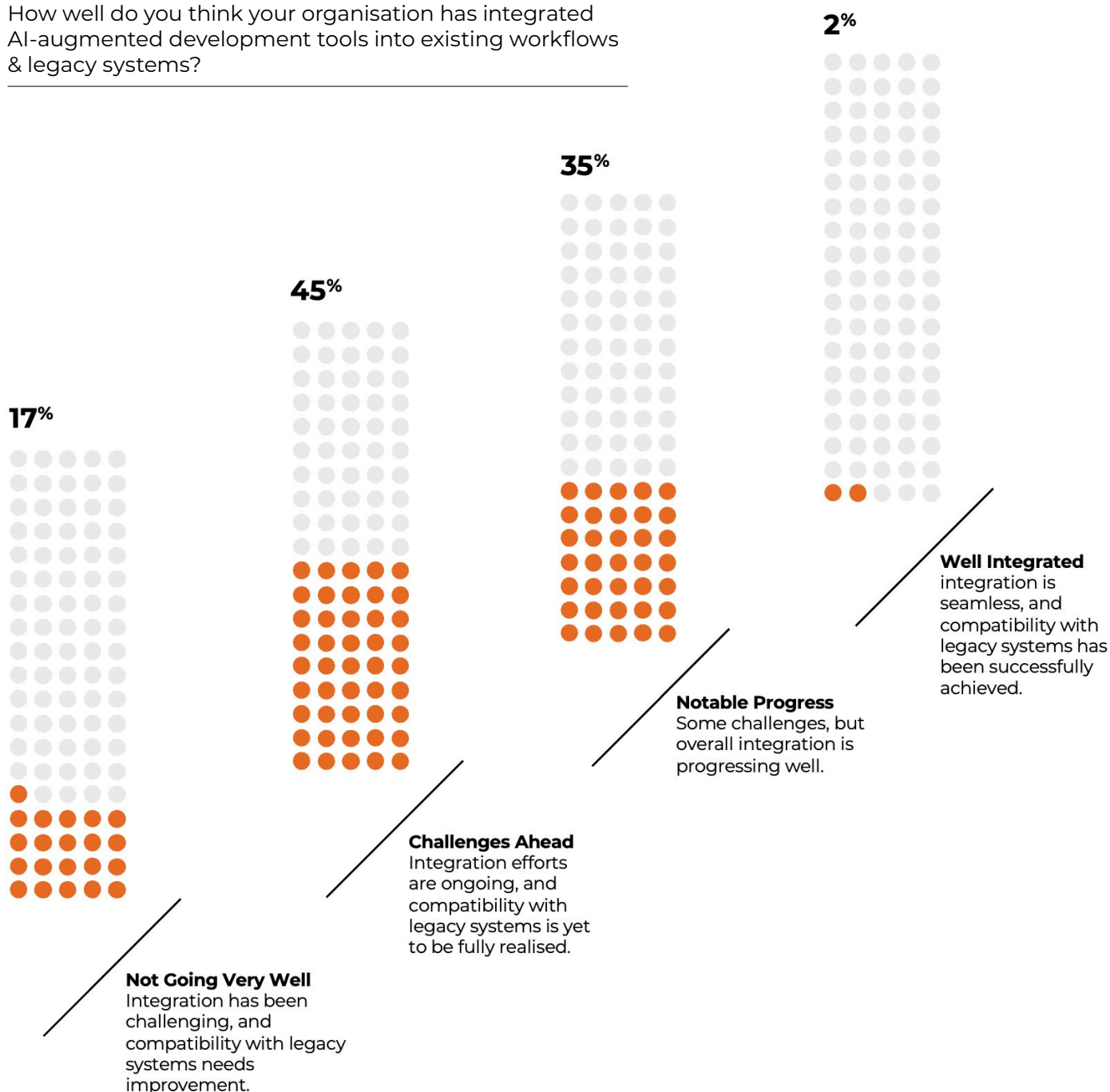


While the potential for AI co-pilots in transforming digital app and service development is recognized, the path to effective integration is fraught with obstacles, primarily due to compatibility issues with legacy systems and the need for organizational adaptation.

A significant 55% of respondents are uncertain about the time-saving benefits of these tools, and 9% have even seen development times increase. However, there is a silver lining, with 36% reporting moderate to significant improvements in project delivery speed. This suggests that while AI-augmented tools hold promise for enhancing efficiency, realizing these benefits requires overcoming initial learning curves and integration challenges.

Survey Question:

How well do you think your organisation has integrated AI-augmented development tools into existing workflows & legacy systems?



2c. Catalysing Speed-to-Value: Maximising the Impact of A.I. on Business, Quickly!

Leading enterprise-scale transformation for A.I. can be daunting for any tech leader. Tech leaders essentially have to become skilled change-managers and recruit change-agents to bring their organisation through a cohesive change strategy. SPARK offers a six-step framework to guide tech leaders in driving sustainable enterprise-scale A.I. transformation journeys in their organisations!

SIX STEP FRAMEWORK TO LEAD SUSTAINABLE ENTERPRISE-SCALE A.I. TRANSFORMATION

COPYRIGHT © SPARK (CIO Academy Pte. Ltd.)

- **1 SECURE LEADERSHIP BUY-IN**
Getting the Board on-board, is non-negotiable
Ensure that board leaders are well-educated on the upside of adoption, to provide concerted leadership support over the long-term for strategic investments into A.I.
- **2 PARTNERING THE BUSINESS**
Building the A.I. Use-case Vault
Democratising co-innovation to formulate A.I. use-cases through a design-driven partnership with business stakeholders
- **3 ASSESS DATA & I.T. READINESS**
Future-Proof the Data Management Stack
Trusted data and resilient data infrastructure is key to build trust & adoption. Tech teams must assess readiness in supporting mission-critical A.I. workloads from the front-office to the back-office.
- **4 IDENTIFY CHAMPIONS**
Embraced Shared IT-Business Ownership
Skin in the game should come from both I.T./Data teams and business units. Business-champions ensure joint ownership of outcomes.
- **5 DEMONSTRATE VALUE QUICKLY**
Delivering Quick-Wins
Tech teams should focus on A.I. use cases that rank both highest in business impact ease-of-implementation to achieve proof-of-value, quickly!
- **6 CONTINUOUS GOVERNANCE & TESTING**
Not Set-&-Forget, but Continuous Testing
A.I. is no longer static, but generative. Strong governance with robust feedback loops is key for trust and adoption to keep growing

Survey Question:

What are the TOP 2 investments/ initiatives you believe are the most urgent for enhancing your organisation's readiness and resilience in the face of AI-related challenges?



2d. Addressing Readiness Gaps & Strengthening A.I. Governance

Job augmentation, and not job replacement, is the goal of leaders in developing their teams to become more A.I. ready in the face of an exponentially A.I. led workplace. In the number one spot of most urgent initiatives to build readiness, survey responses emphasised the need for more training

and talent development programmes. This recognizing the pivotal role that skilled personnel play in navigating the complexities of A.I. and underscores a growing awareness of the need for human-centric strategies to harness the potential of A.I. effectively.

On October 30, 2023, the White House issued a wide-ranging executive order establishing a framework for regulation of A.I.. The executive order aims to support the development of A.I. and promote innovation and competition, while establishing safeguards to minimize the risks of the new technology. The EU has followed closely with the introduction of the A.I. Act to manage risks associated with A.I. applications, emphasizing transparency and accountability. With the regional and in many cases, global nature of business, disparate regulatory standards will drive up cost of compliance quickly and challenge the economics of A.I. adoption at scale. Hence, close engagements with regulatory institutions and certifications bodies will aid greatly to enable global harmonisation of standards and collectively reduce compliance costs in the future.

Unlike previous technologies, A.I.'s adaptive and self-learning nature introduces complexities that demand a proactive stance to govern both the underlying models and technologies, but also the data management systems and processes to enhance data trust and maintain a high degree of data integrity. Regular assessments and scenario planning exercises emerge as essential tools for organisations to stay agile and responsive in anticipating and mitigating emerging risks.

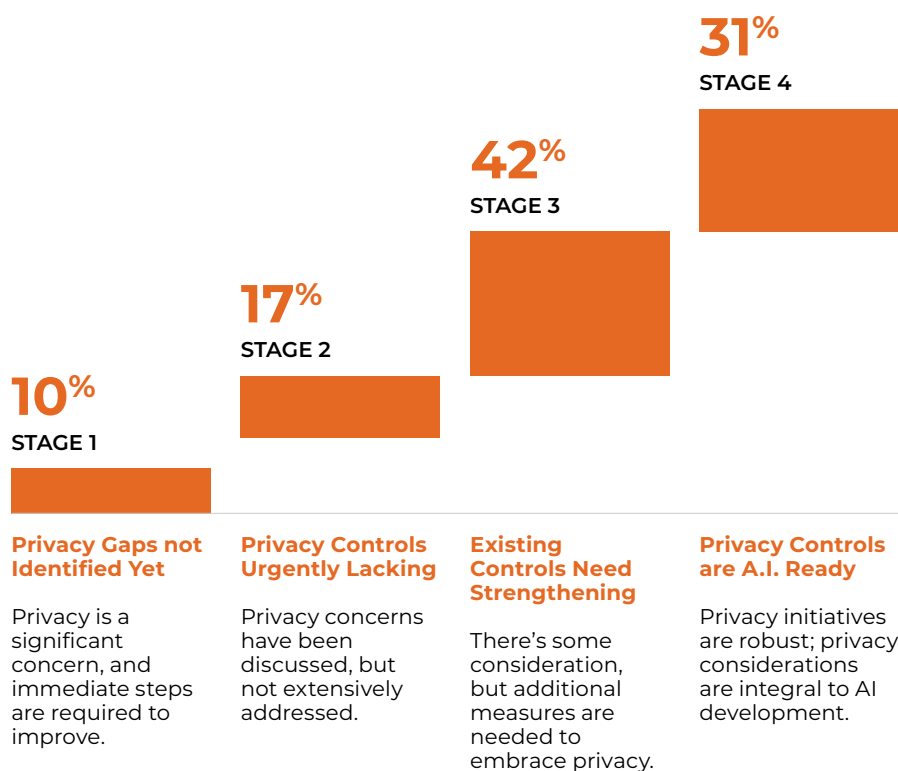
The US and European Union (EU), have taken the initial steps to offer a flavour of global standardisation in frameworks and guidelines for A.I. risk management, riding on existing standard-setting bodies, such as the A.I. Risk Management Framework Playbook ((A.I. RMF1.0) published by the National Institute of Standards and Technology (NIST) from the US Department of Commerce, the EU Artificial Intelligence Act, in which the first draft of the final policy paper is ready for public view. Singapore has also taken a proactive approach, with the establishment of A.I. Trust, Risk, and Security Management (A.I. TRiSM) framework and the A.I. Verify Programme by the Singapore Infocomm Media Development Authority (IMDA), which is designed to promote responsible A.I. usage by providing a verifiable testing process for industry players. It aims to enhance transparency in A.I. systems, build trust with stakeholders, and contribute to the development of international standards on A.I. governance.

Segment 3:

Fostering Data Trust, Strengthening Data Ownership & Defending Data Privacy

Survey Question:

To what extent do you believe privacy concerns are adequately addressed within existing AI initiatives in your organisation?



3a. Room to Strengthen Data Privacy ahead of Growing A.I. Footprint in the Enterprise

From our latest survey, just over 2 out of 3 organisations have some ways to go for strengthening privacy policy controls ahead of enterprise-wide A.I. adoption. The rapid adoption of enterprise-grade generative A.I. tools, such as co-pilots, can pose data exposure risks to third-party vendors due to the potential leakage of sensitive information. To mitigate these risks and enhance data privacy governance policies, organisations can adopt the following strategies:

Implement Robust Data Protection Measures:

Organisations should enforce stringent data protection measures, including encryption of data in transit and at rest, to safeguard sensitive information from unauthorized access during interactions with third-party vendors. Utilising technologies like tokenization, anonymization, and fully homomorphic encryption can help protect data privacy while enabling secure collaboration with external partners.

Establish Clear Data Sharing Protocols:

Define clear data sharing protocols and access controls to regulate the flow of information shared with third-party vendors, especially with the use of generative A.I. tools. Implementing role-based access controls and monitoring data transfers can help prevent unauthorized data exposure. Incorporating privacy-by-design principles

into data sharing processes helps ensure that privacy considerations are embedded from the outset, promoting responsible data handling practices. Often, companies are forced to balance zero-sum trade-offs between functionality and privacy. As such, careful design of customer and user experiences through robust product management processes and extensive governance of personal data, will be imperative to achieve the best of both worlds.

Enhance Collaboration and Transparency:

Foster collaboration across legal, risk management, and data governance teams to develop comprehensive A.I. governance programs that outline guidelines for responsible A.I. usage and data sharing practice. Promote transparency by disclosing the use of A.I. tools in data processing, informing individuals about how their data is utilized, and providing mechanisms for data access, deletion, or opt-out options to enhance user control over their personal information. By adopting these strategies, organisations can mitigate data exposure risks associated with enterprise-grade generative A.I. tools when interacting with third-party vendors. Strengthening data privacy governance policies and processes is essential to uphold privacy standards and build trust with stakeholders.

3b. Room to Strengthen Data Trust ahead of Growing A.I. Footprint in the Enterprise

A survey done by Salesforce, showed that 45% of consumers surveyed do not trust companies to use A.I. ethically, with the World Economic Forum (WEF) citing “**lack of transparency and explainability**” as one of the top three challenges hindering the societal adoption of A.I.. (World Economic Forum, 2023).

Interpretability and transparency are critical to building trust in your organisation’s A.I. implementations. The top two most urgent measures, “**Implement Explainable A.I. Techniques & Tools for Better Interpretability**” and “**Establish Clear Communication Channels to Educate Stakeholders about A.I. Processes,**” both emphasize the need

for demystifying the inner workings of new and existing A.I. systems.



Only 4.5 in 10 Consumers Trust Companies to Use A.I. Ethically

Source: State of the Connected Customer Report, Salesforce

Furthermore, the survey’s third most urgent measure, “**Develop a transparent A.I. governance framework with public input,**” underscores the need for establishing clear ethical guidelines and involving stakeholders in the development and deployment of A.I. projects. This echoes the growing call for **responsible A.I. development** practices that prioritize fairness, accountability, and human oversight. By prioritizing these measures,

your organization can demonstrate its commitment to building trust with both internal and external stakeholders in the evolving landscape of A.I..

Recommended framework for A.I. governance:

Foundation Building

1. **Lawfulness:** Trustworthy A.I. systems must comply with relevant laws and regulations, including data protection laws like the European General Data Protection Regulation (GDPR) and domain-specific rules in high-risk sectors such as healthcare or finance

2. **Ethics:** In addition to legal compliance, trustworthy A.I. systems should adhere to ethical principles and values. This layer addresses ethical dilemmas arising from rapid technological advancements in A.I. systems, ensuring that ethical considerations are integrated into A.I. development and deployment.

3. **Robustness:** Trustworthy A.I. systems should operate safely and reliably, ensuring they do not cause unintentional harm. This pillar focuses on technical performance, reliability, and social suitability of A.I. systems to guarantee their robustness from both technical and social perspectives.

Survey Question:

Which of the measures is most urgent to enhance trust in your organisation's AI implementations?

#1



Implement **Explainable A.I.** Techniques & Tools for Better Interpretability

#2

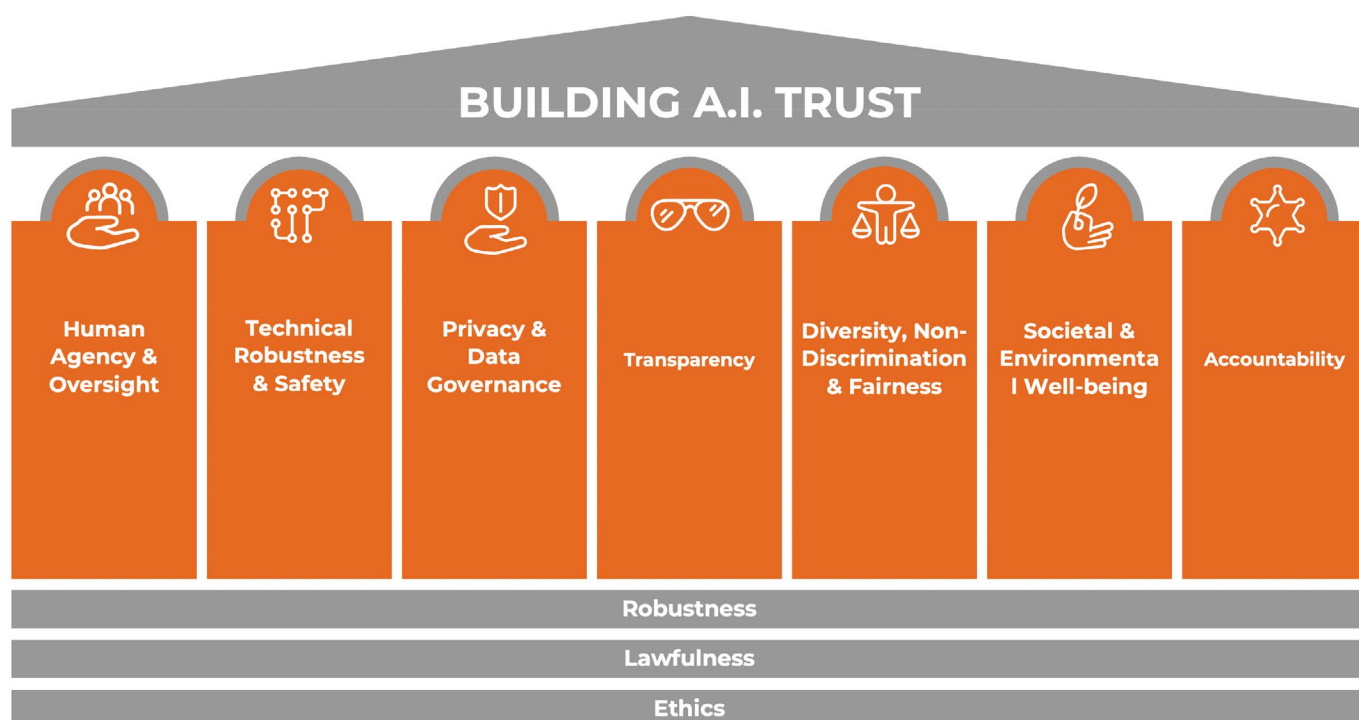


Establish Clear Communication Channels to **Educate Stakeholders** about A.I. Processes.

#3



Develop a **transparent A.I. governance** framework with public input.



Key Pillars of Trust Building

- 1. Human Agency and Oversight:** A.I. systems should empower individuals to make informed decisions while ensuring proper oversight mechanisms are in place. Human-in-the-loop and human-on-the-loop approaches can enhance human control over A.I. systems, fostering fundamental rights and accountability.
- 2. Technical Robustness & Safety:** Ensuring performance, reliability, and confidence in A.I. systems is crucial to foster trustworthiness for A.I. workloads to be embedded into mission-critical business operations.
- 3. Privacy & Data Governance:** Respecting privacy rights and implementing robust data governance practices throughout the A.I. system's life cycle is essential. Adequate data governance mechanisms ensure data quality, integrity, relevance, and legitimate access while protecting privacy.
- 4. Transparency:** Transparency involves sharing appropriate information with stakeholders, ensuring explainability of A.I. decisions, and communicating the capabilities and limitations of A.I. systems openly.
- 5. Diversity, Non-discrimination & Fairness:** Reducing unfair bias, fostering diversity, ensuring accessibility for all individuals regardless of disability, and involving stakeholders throughout the A.I. system's life cycle. By promoting fairness and non-discrimination, this pillar aims to ensure that A.I. systems do not deceive humans or restrict their freedom of choice unjustly.
- 6. Societal & Environmental Well-being:** Objective evaluation of the implications of A.I. on sustainability goals and ensuring that A.I. development aligns with societal well-being and environmental sustainability.
- 7. Accountability:** Meticulous attribution of ethical and legal responsibility for decisions and actions made by A.I. systems to human actors. It ensures that individuals or entities can be held accountable for the outcomes of A.I. systems at any stage of their life cycle, promoting transparency and ethical conduct in A.I. development and deployment.

3c. A.I. Defines the new Battle Ground for Cyber Warfare

The recent findings from our survey and the latest data gleaned in reference to the MITRE ATT&CK framework, highlight a complex and evolving landscape of cyber threats and vulnerabilities, particularly in the realm of protecting data in organisations. The key findings can be categorized into top tactics, techniques, and procedures (TTPs), emerging threats and vulnerabilities, and best approaches for strengthening defenses.

2022 ► 2023

333% INCREASE IN CYBER-ATTACKS



Top Tactics, Techniques & Procedures (TTPs)



Advanced Persistent
Campaigns



Credential Theft
& Privilege Escalation



Ransomware
/ Malicious Encryption

176% INCREASE IN DATA EXFILTRATION TACTICS

Application of Stealth Tactics



Stealthy Process
Injection



Disabling Cyber-alerts
by Obfuscation



Deepfakes & Social
Engineering

Top Tactics, Techniques, and Procedures (TTPs)

The identified top TTPs include Advanced Persistent Campaigns, Credential Theft & Privilege Escalation, Ransomware, and Malicious Encryption. These tactics are further complemented by applications of stealth tactics such as Stealthy Process Injection, Disabling Cyber-alerts by Obfuscation, Deepfakes, and Social Engineering. For instance, the LAPSUS\$ group's activities exemplify the use of legitimate tools for credential harvesting and privilege escalation without deploying malware, highlighting the sophistication of current threat actors.

A.I. plays a pivotal role in enabling sophisticated social engineering attacks, particularly through the use of deepfakes and identity theft. These advancements in A.I. technology have significantly enhanced the capabilities of cybercriminals, allowing them to create hyper-realistic impersonations and manipulate digital content for malicious purposes.

Deepfakes in Social Engineering

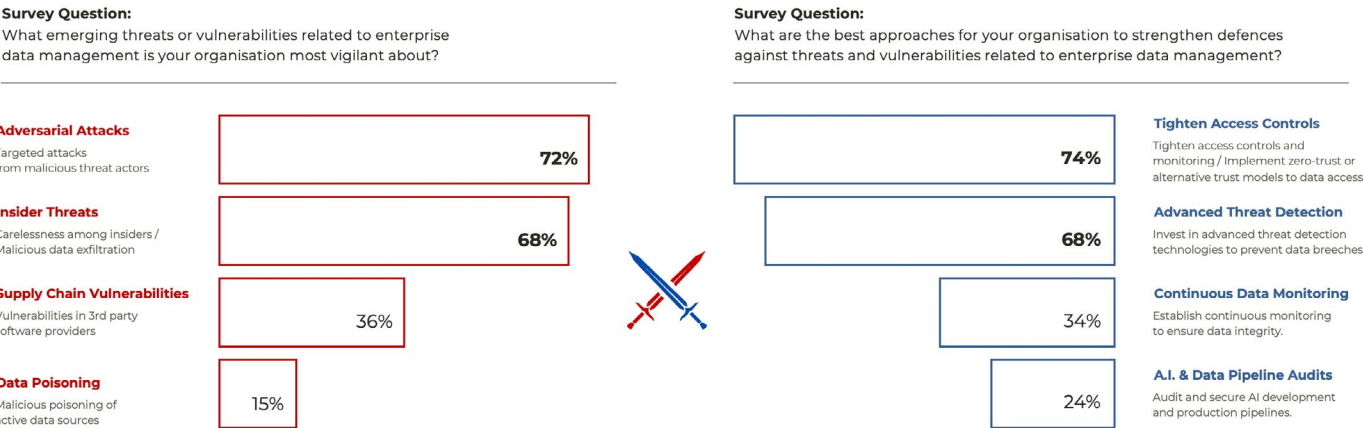
Deepfake technology represents a pinnacle of A.I. sophistication, enabling attackers to manipulate videos and audio to create hyper-realistic impersonations of individuals. This technology allows cybercriminals to fabricate convincing content, such as video messages from CEOs requesting funds transfers or confidential data, which can

deceive targets into taking actions that compromise security. The rise of deepfakes poses significant challenges for verification and trust, as A.I.-generated content becomes increasingly indistinguishable from reality, making it difficult for individuals and organizations to discern genuine communications from fraudulent ones.

A.I.'s adaptive nature enhances the sophistication and efficiency of social engineering attacks by automating target profiling, efficient information gathering, and personalization for deception. Through machine learning algorithms specialized for pattern recognition and data analysis, A.I. can swiftly scrape data from various sources to gather comprehensive information about potential targets. This automation streamlines the reconnaissance phase of social engineering attacks and enables the creation of highly personalized phishing emails based on the collected data. Moreover, A.I.'s learning algorithms allow it to adjust tactics based on the success or failure of previous attempts, enhancing its effectiveness in manipulating targets.

In addition, Generative A.I. tools are being used to support identity theft and fraud by creating realistic deepfakes that can bypass facial matching and liveness detection in ID document verification processes. Fraudsters now have the ability to cheaply produce highly authentic images and videos that closely resemble their desired targets within seconds, enabling them to deceive systems relying on biometric authentication or identity verification measures. What is particularly dangerous to regulated industries, are new generative A.I. solutions utilised to create synthetic identities with realistic identification numbers, which are then used for illegal activities like creating fake bank accounts or applying for government benefits.

3d. Most Urgent Threats & Vulnerabilities and Most Urgent Countermeasures



Emerging Threats and Vulnerabilities

Organisations are most vigilant about adversarial attacks and targeted attacks from malicious threat actors (72%), insider threats including carelessness and malicious data exfiltration (68%), followed by supply chain attacks (36%) and data poisoning (15%). These concerns are validated by the observed activities of threat groups like Blind Eagle and the prevalence of ransomware affecting critical infrastructure, as reported by BlackBerry.

Best Approaches for Strengthening Defences

To counter these threats, organizations are investing in advanced threat detection technologies (65%), tightening access controls and implementing zero-trust models (74%), establishing continuous monitoring of data integrity (34%), and securing A.I. development pipelines (24%). These strategies are supported by best practices such as enhancing data protection and management, employing biometric security, and simplifying technology infrastructure to prevent cyber-attacks.

The convergence of sophisticated TTPs with emerging threats like deepfakes and A.I.-driven attacks necessitates a multifaceted approach to cybersecurity. The emphasis on advanced threat detection technologies and zero-trust models reflects a shift towards proactive and dynamic defense mechanisms. However, the relatively low focus on continuous monitoring of data integrity and securing A.I. pipelines suggests potential areas for improvement, given the increasing reliance on A.I. and the proliferation of insider threats.

The findings underscore the importance of not only technological solutions but also organizational and human factors in cybersecurity. Insider threats, whether due to carelessness or malice, highlight the need for comprehensive security awareness training and robust access management policies. Similarly, the threat of data poisoning emphasizes the need for stringent data validation and monitoring practices, especially in A.I.-driven systems.

Defending against the current and emerging cybersecurity threats requires a holistic approach that combines advanced technologies, stringent access controls, continuous monitoring, and human-centric strategies. Organizations must remain vigilant and adaptable, continuously evolving their cybersecurity practices to address the complex and dynamic threat landscape.

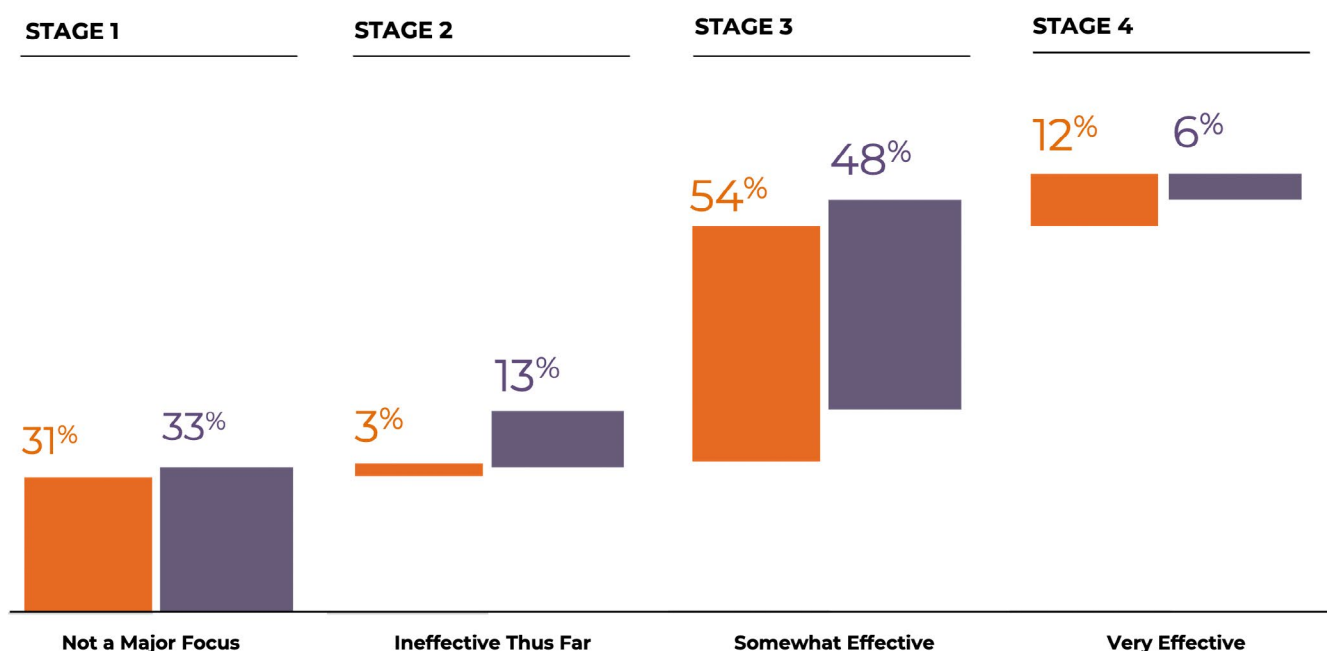
Segment 4:

Building a Sustainability-Conscious Technology Organisation

Survey Question:

How would you rate your organisation's current efforts in measuring and tracking the environmental footprint of IT initiatives?

To what extent do you believe software development teams are effective in integrating sustainable practices, to minimise resource consumption and optimise code efficiency?



Our latest findings provide a nuanced view of how organizations perceive their efforts in environmental sustainability within IT initiatives and software development practices.

Environmental Footprint of IT Initiatives

Only 12% of organizations rate their efforts as very effective in measuring and tracking the environmental footprint of IT initiatives, indicating a significant gap in robust measurement mechanisms. For example, TechTarget's recent survey showed a full 89% of organizations recycle less than 10% of their IT hardware, and only 43% of executives are aware of their organization's IT footprint.

Furthermore, despite 50% of companies having an organisation-wide sustainability

strategy, only 18% possess a complete sustainable IT strategy with clear goals and timelines. Which is also reflected in our Asia focused data, with 1 in 3 companies not pursuing sustainability-conscious procurement practices for I.T. resources at the moment.

Sustainable Practices in Software Development

When it comes to integrating sustainable practices in software development, only 6% of organizations believe they do so very effectively. Green coding practices represent not just a trend but a fundamental shift in the ethos of software development today. New practices such as energy-efficient coding, optimized algorithms, and sustainable design principles, are crucial for minimizing resource consumption and optimizing code efficiency, especially more resources deployed into A.I. workloads. In Asia, we observe significant room for improvement, with 48% of organisations acknowledging awareness but noting that improvements can be made to current development practices.

Low-Hanging Fruits to Achieve Quick-Wins for Sustainability



Optimise Data Center Operations

Transition toward Virtualisation & Cloud



Recycle I.T. Hardware

Adopt recycling or upcycling practices as part of hardware end-of-life treatment policies



Adopt Green Coding Practices

Efficient code and monitoring of resource consumption patterns of software applications



Implement Power-Saving Practices

On-premise devices can be set to power down after periods of inactivity



Embed Sustainability Metrics

Procurement frameworks today should include sustainability metrics in vendor selection



Tier Data Storage & Workload Up-Time

Implementing a mix of "hot" and "cold" storage, and workload tiering based on business need, goes a long way and saves significant cost too

1. Optimize Data Center Operations

Virtualization and cloud computing reduce the need for physical servers, cutting down on energy use and hardware waste. Cloud providers often use more energy-efficient data centers, sometimes powered by renewable energy.

2. Recycle IT Hardware

Recycling or upcycling IT hardware prevents environmental waste and reduces the demand for new raw materials. It also supports resource conservation and can provide cost savings.

3. Adopt Green Coding Practices

Green coding practices ensure software runs efficiently, using less energy. Monitoring resource consumption helps in optimizing code performance and reducing carbon footprint.

4. Implement Power-Saving Practices

Devices set to power down during inactivity save energy. This simple measure can lead to substantial reductions in energy consumption.

5. Embed Sustainability Metrics in Procurement

Incorporating sustainability metrics into vendor selection encourages eco-friendly supply chain practices. This approach aligns procurement with environmental sustainability goals.

6. Tier Data Storage & Workload Up-Time

Using a mix of “hot” and “cold” storage optimizes energy consumption based on data access needs. Workload tiering aligns server activity with business requirements, saving energy and costs.

Challenges and Opportunities

The challenges in both measuring the environmental footprint of IT initiatives and integrating sustainable practices in software development are multifaceted. They include the complexity of tracking digital carbon footprints, the scattered nature of sustainability data across departments, and the gap between the desire to implement green practices and the actual execution. Moreover, the lack of common standards for measuring IT carbon footprints exacerbates these industry head-winds.

On the other hand, the pursuit of sustainability in software development presents opportunities for innovation, cost savings, and alignment with Corporate Social Responsibility (CSR) goals. By adopting green coding practices, organizations can not only reduce their environmental impact but also foster a culture of sustainability that permeates corporate strategies and operations.

There is a clear and urgent need for organisations to enhance their efforts in measuring and tracking the environmental footprint of IT initiatives and integrating sustainable practices in software development. While there are significant challenges, the opportunities for innovation, cost savings, and environmental stewardship are equally compelling. Organisations must prioritize the development of robust measurement mechanisms, adopt common standards for tracking IT carbon footprints, and fully integrate sustainable coding practices to navigate the complexities of sustainability in the digital age.

Citations:

<https://research.nccgroup.com/2022/04/28/lapsus-recent-techniques-tactics-and-procedures/>
<https://www.blackberry.com/us/en/solutions/threat-intelligence/2023/threat-intelligence-report-april>
<https://www.getgsi.com/blog/top-10-emerging-cybersecurity-threats>
<https://www.ekransystem.com/en/blog/best-cyber-security-practices>
<https://www.linkedin.com/pulse/evolution-tactics-techniques-procedures-ttps-warfare-guy-horesh-gunin-04j6f>
<https://www.csoononline.com/article/571455/how-deepfakes-enhance-social-engineering-and-authentication-threats-and-what-to-do-about-it.html>
<https://www.linkedin.com/pulse/navigating-cybersecurity-landscape-future-risks-mitigation-kale>
<https://www.cynet.com/network-attacks/privilege-escalation/>
<https://arxiv.org/pdf/2306.13033.pdf>
<https://www.hpe.com/us/en/what-is/ai-security.html>
<https://www.mdpi.com/2227-7390/11/14/3115>
<https://zvelo.com/the-role-of-ai-in-social-engineering/>
<https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/>
https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf
<https://decoded.avast.io/threatresearch/avast-q3-2023-threat-report/>
<https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030/@@download/fullReport>
<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10145335/>
<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullReport>
<https://www.linkedin.com/pulse/emerging-threats-software-supply-chain-attacks-deepa>
<https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf>
<https://www.varutra.com/ctp/threatpost/postDetails/Security-Vulnerability-in-WinRAR-Allows-Hackers-to-Execute-Programs-via-Opening-RAR-Archives/Zjk4V1hxdmhTYWpxYVJzTWtzVldGQT09>
<https://www.xenonstack.com/blog/machine-learning-security>
<https://www.exabeam.com/information-security/cyber-security-threat/>
<https://research.nccgroup.com/2021/05/04/rm3-curiosities-of-the-wildest-banking-malware/>
<https://www.leewayhertz.com/data-security-in-ai-systems/>
<https://www.techtarget.com/searchcio/feature/Understand-the-digital-carbon-footprint-of-enterprise-IT>
<https://www.linkedin.com/pulse/sustainable-coding-greener-approach-software-moureen-milgo-vjxuf>
<https://irisarbon.com/esg-reporting-in-2024-the-imperative-for-sustainable-corporate-practices/>
<https://sustainablefuturenews.com/esg/esg-and-sustainability-reporting-the-essential-guide-for-2023-2024/>
<https://www.forbes.com/sites/bernardmarr/2023/03/22/green-intelligence-why-data-and-ai-must-become-more-sustainable/?sh=58d2cc867658>
<https://www.techtarget.com/searchsoftwarequality/tip/Green-coding-best-practices-and-how-to-get-started>
<https://www.internationalaccountingbulletin.com/sponsored/ai-software-esg-reporting/>
<https://facilio.com/blog/sustainability-reporting-frameworks/>
<https://www.persefoni.com/learn/emissions-management-software>
<https://fullscale.io/blog/software-development-in-2024-trends/>
<https://www.coolset.com/academy/sustainability-predictions>
<https://fiscalnote.com/blog/top-esg-trends-2024>
<https://www.brightest.io/sustainability-reporting-standards>
<https://www.erlang-solutions.com/blog/the-future-trends-of-sustainability-in-programming-software/>
<https://www.ironhack.com/us/blog/sustainability-in-tech-how-green-practices-are-shaping-the-industry-in-2024>
<https://www.mobilexpense.com/en/blog/future-of-carbon-tracking-in-europe-best-practices-key-trends>
<https://www.linkedin.com/pulse/future-software-development-trends-watch-2024-quickwayinfosystems>
<https://aplanet.org/resources/sustainability-and-csr-trends/>
<https://greenly.earth/en-gb/blog/ecology-news/everything-you-need-to-know-about-green-it-in-2022>
<https://www.moontechnolabs.com/blog/software-development-best-practices/>
<https://www.mnp.ca/en/insights/directory/risk-trends-2024-environmental-social-and-governance-esg>
<https://www.artefact.com/blog/use-data-to-measure-and-reduce-your-environmental-impact-with-artefact/>
<https://www.linkedin.com/pulse/new-upcoming-climate-reporting-legislation-watch-2024-harun-tasci>
<https://www.coolset.com/academy/top-carbon-accounting-software-tools>
<https://www.gartner.com/en/articles/are-you-thinking-too-small-about-sustainable-technology>