

CMA DIGEST

December 2025, Issue - 110, Volume 64

ED VOICE – From the Editor's Desk

Dear Readers,

Greetings from the desk of "CMA Digest". As we near the end of 2025, we are grateful for your continued patronage of our newsletter.

As this year draws to a close, it is time to introspect on the year gone by, and set new goals for the upcoming year. 2025 continued to witness global unrest with multiple wars and continuing conflicts. Despite this, India did manage to perform well, and it is hoped that it will emerge to be in the top three economies of the world.

December 2025 was a routine month for CMA, with the popular "Monday Musings" series going on in full steam. Many exciting programs are slated for the next two months, and these will be reported in details in our future editions.

See you all again in 2026!

Mr. K. Seetharam

Editor
CMA Digest



Editorial Team

Mr. K. Seetharam | Dr. A.G.V. Narayanan
Mr. N. Krishna Kumar | Dr. D.K. Karthikeyan
Dr. Vandana Madhavkumar | Ms. S. Sujithra Vadivu



COIMBATORE MANAGEMENT ASSOCIATION

Monday Musings

Monday Musings – 01st December 2025

Speaker: **Mr. Abishek Ravichandran**

Strategic Cannibalization: Why Great Companies Kill Their Own Products Before Competitors Do

The session was titled “Strategic Cannibalization: Why Great Companies Kill Their Own Products before Competitors Do.” The presentation focused on the critical leadership mind-set necessary for proactive self-disruption and explored how global industry leaders such as Apple, Amazon, and Netflix successfully transformed themselves by intentionally cannibalizing their own profitable products to sustain market dominance.

The presentation also highlighted the decline of once-powerful companies like Kodak, Nokia, and BlackBerry, demonstrating that

organisations that resist reinvention ultimately risk irrelevance and collapse.

Through real-world case studies, strategic frameworks, audience polls, and interactive discussion, the session encouraged future managers, entrepreneurs, and academic professionals to embrace innovation-led thinking, agility, and bold decision-making as essential drivers of long-term organisational survival and success.



Monday Musings – 8th December 2025

Speaker: **Dr. K. V. Manju**

Career 2.0: Succeeding When AI Becomes Your Co-Worker

Dr. K. V. Manju, Associate Professor, School of Management, Sri Krishna College of Engineering and Technology, Coimbatore, delivered a talk on “Succeeding When AI Becomes Your Co-Worker”, which was an insightful presentation on the future of work, skills, and human–AI collaboration, presented by Dr. K. V. Manju, Associate Professor, Sri Krishna College of Engineering and Technology.

The session began by drawing attention to how deeply AI already influenced everyday work and addressed the common concern that artificial intelligence might threaten jobs. Dr. Manju explained the shift from Career 1.0 to Career 2.0, where AI had evolved from being a simple tool to becoming a partner in the workflow. Through interactive discussions and the Human or AI quiz, participants explored how routine and repetitive tasks could be handled by AI, while humans continued to play a critical role in judgment, negotiation, ethics, and final decision-making. The presentation further introduced the 3-Buckets Exercise to help

participants classify tasks as automatable, augmentable, or human-exclusive, supported by global evidence showing that a significant portion of corporate work was already automatable. Case examples from Infosys and Amazon demonstrated how AI-driven automation had reshaped hiring and work design rather than eliminated jobs, reducing the need for certain low-skill tasks while creating new roles in areas such as robotics maintenance, quality assurance, safety management, data operations, and process optimization.

The session concluded by highlighting irreplaceable human strengths such as creativity, empathy, critical thinking, and leadership, and by outlining a practical Career 2.0 roadmap and 30-day upgrade plan. The key takeaway emphasized that the future of work lay in combining human strengths with AI speed, enabling professionals to remain relevant and resilient in an AI-driven world.



Monday Musings – 15th December 2025

Change Management in a multipolar world

Dr. C. N. Narayana, in his session of the captioned topic, covered various aspects of change management and critical factors which are making the change faster than ever in the ever-changing world. He used the 7 R factors for change which drives the change. He emphasized the need for open communication, embracing technology including AI and beyond. He also shared his practical experience in multinational and Indian organizations regarding resistance to change and how successful leadership handles situations in organizational development through change management process. He also shared his views on Gen Z and their mental health issues while handling change process and steps to ensure adaptation and sustainability. He enumerated at length regarding radical changes happening globally and how it affects all the stakeholders irrespective of the geography we belong to and

Speaker: **Prof. C.N.Narayana**

the challenges faced. He also shared the concept of ADKAR (Awareness, Desire, Knowledge, Ability, and Reinforcement) with a resilient attitude towards radical changes.

He also covered three main pillars of change namely Operations and process, Customer Experience, and New Business Models. He summarised the session with the metaphors of change from a caterpillar to a butterfly, which is both a fantasy and a painful process. A structured approach guiding teams and organizations can lead to transformational change achievement as a whole. It was an insightful session to all management practitioners, students, and professionals.

Monday Musings – 22nd December 2025

Value Education

The speaker, Ms. Pritaa K, stressed that value education was something more important than marks, degrees, designations, and salary. She defined education as transmission of knowledge, skills, methods, and formulas in a structured curriculum, whereas value education is not about preaching morals, but about thinking what kind of person one should become. It is about answering quietly to ourselves what our mind carries.

Value education matters today, especially in a fast-changing world in terms of AI, robotics, automation, etc. On the down side, we are seeing a rapid rise of stress and anxiety, growing conflicts and corruption, an education system that creates knowledgeable minds but empty hearts. Value education is not about teaching lessons, but about building character.

She quoted Dr. Kalam, who said: "Knowledge makes you great; values make you good." Values are not taught by words - they are revealed through small actions.

She stressed on the core values for life, namely:

1. Honesty & Integrity: Integrity means doing the right thing even

Speaker: **Ms. Pritaa K**

when no one is watching.

2. Respect: Respect for parents, teachers, colleagues, and the environment.

3. Responsibility: Owning mistakes, duties, performance.

4. Compassion: Be Kind to people around you even to the unknown.

5. Discipline: Discipline is doing what is needed, not what is easy.

6. Gratitude: Being thankful creates positivity.

She advised the audience to start practicing any one value from the next day onwards - Speaking the truth, showing compassion, helping someone, forgiving someone, being patient, respecting others, saying "thank you", or protecting the environment.

She concluded her talk by stating that education makes one capable, but values make one valuable. If we all practice small values daily, we create a better family, better workplace, better community, and a better world.

Monday Musings – 29th December 2025Speaker: **Mr. B. Bala Senthil Kumar**

Career 2.0 - Master the Career skills

The Career 2.0 session was designed to guide students and young professionals towards meaningful and sustainable career paths, with a strong focus on Public Sector Services and Central Government opportunities. In an era of rapid change, government careers continue to offer stability, respect, growth, and long-term impact. This session highlights opportunities in Banking, Insurance, SSC, UPSC, Railways, Defence, and other central services, while helping participants understand eligibility, preparation strategy, and long-term career vision.

Beyond opportunities, Career 2.0 emphasizes core skill development that determines success across all competitive exams and professional journeys. Special focus is given to quantification skills, helping students strengthen numerical aptitude, logical thinking, and problem-solving ability. Self-awareness is addressed

to help learners identify their strengths, interests, and realistic career fit instead of blindly following trends.



The session also stressed on Time Management, teaching participants how to balance academics, exam preparation, and personal growth through structured routines and smart prioritization. A unique concept, "Going Small," encourages students to break big goals into small, consistent actions—daily habits that compound into long-term success.

Overall, Career 2.0 is not just about exams, but about building clarity, discipline, confidence, and a future-ready mind-set for lifelong career growth.

Management Quiz

- Q1. FutureMe, an ultra-luxury skin-care brand recently introduced in India, was first launched in which country?
- Q2. Where is The House of FutureMe, the brand's experience centre, located in India?
- Q3. Coursera has announced the acquisition of which peer platform in an all-stock deal?
- Q4. Name a few companies which are into 10-minute house-help service firm?
- Q5. Reliance Consumer Products Limited entered the packaged foods segment by relaunching which legacy brand?
- Q6. COTPA stands for _____
- Q7. Honasa Consumer's acquisition of BTM Ventures enables its entry into which segment?
- Q8. Reliance Consumer Products Limited acquired a 70% stake in which Tamil Nadu-based company?



For answers see page 07

Emerging Cyber Security Trends in 2026:

AI, Identity, and the New Attack Frontier

INDUSTRY 4.0[®]
Fostering Manufacturing

WE COVER LATEST TECHNOLOGIES AND TRENDS IN MANUFACTURING



Emerging Cyber Security Trends in 2026

Source : <https://industry4o.com>

As we are nearing 2026, the cyber security landscape is undergoing rapid evolution, fuelled by technological advancements, emerging AI transformation and increasingly sophisticated cyber threats. Let's dive into the most notable emerging trends in cyber security for 2026, emphasizing the profound impact of Artificial Intelligence (AI), the crucial importance of identity management, and the expansion of the attack surface into previously unexplored areas.

Technological innovation is reshaping the fabric of cyber security. Artificial intelligence, machine learning, quantum computing, and the proliferation of connected devices are revolutionising both defensive and offensive capabilities. While these advances offer remarkable opportunities for automation, threat detection, and rapid response, they also introduce new vulnerabilities and attack vectors. The pace of change demands that cyber security teams remain agile, continually updating their skills and tools to keep pace with the latest developments.

The future of cyber security extends beyond traditional boundaries. Organisations must proactively address emerging risks such as quantum threats, deep-fake technologies, and the exploitation of artificial intelligence. Additionally, the regulatory landscape is evolving, with stricter data privacy laws and

compliance requirements. Proactive risk management, regular security assessments, and investment in employee training will be essential to staying ahead of the curve and building organisational resilience.

The Rise of Artificial Intelligence in Cyber Security

Artificial intelligence has emerged as a double-edged sword in the realm of cyber security and that has been discussed frequently across all round tables. On one side, AI-powered tools are significantly enhancing the capabilities of defenders, enabling them to detect, analyse, and respond to threats with uncommon speed and precision. Machine learning models can sift through massive datasets to identify anomalies, automate incident responses, and even predict future attacks based on historical data. On the contrary, cybercriminals are exploiting AI to automate their attacks, increase the identity, create highly convincing phishing campaigns, and evade traditional security measures.

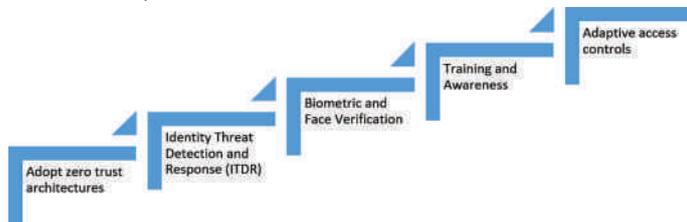
Looking ahead to 2026, we anticipate a notable increase in the deployment of AI-driven security solutions, including autonomous threat hunting, intelligent deception technologies, and adaptive authentication systems. However, this advancement also necessitates heightened vigilance against AI-generated threats, such as deep-fake-based social engineering and AI-assisted

malware. As AI continues to evolve, both defenders and attackers will need to adapt their strategies to navigate this rapidly changing landscape.

Identity as the New Perimeter

In the era of cloud computing and distributed workforces, the concept of a fixed network perimeter has lost its significance. Instead, identity around users, devices, and service accounts has emerged as the central pillar of enterprise security and adapting to zero trust. Malicious actors increasingly target credentials and identity systems, recognising that breaching identity controls can grant access to a wide array of resources to influence. As a result, robust identity protection is now vital, and with digital identity serving as the gateway to critical information, applications, and infrastructure, the need for investing time and effort on this area has become the emerging demand in this new threat landscape.

Some of the places to invest includes –



Biometric authentication, face identity verification, behavioural analytics, and adaptive access controls will become more prevalent, aiming to minimise the risk of credential theft and account compromise. The focus will shift from defending networks to safeguarding digital identities, with increased investment in identity threat detection and response (ITDR) solutions.

By embracing these measures, cyber-security professionals and IT leaders can position their organisations to meet the evolving challenges of a perimeter less digital world, safeguarding assets and ensuring operational resilience well into 2026 and beyond.

The Expanding Attack Surface: New Frontiers

The digital landscape is undergoing a rapid transformation, driven by the propagation of Artificial Intelligence, Internet of Things (IoT) devices, the integration of Operational Technology (OT), and the emergence of smart infrastructure. As organisations accelerate their adoption of these technologies, the digital attack surface is increasing with potential vulnerabilities that expands dramatically.

For cyber-security professionals and IT leaders, this evolution presents both unprecedented opportunities and urgent challenges, as adversaries exploit new vectors to target critical systems and infrastructure. Moreover, the convergence of cyber

and physical security means that attacks may have substantial, real-world impacts. For example, ransomware targeting bank systems, healthcare platforms, and autonomous vehicles is raising severe consequences for public safety and trust.

Some of the key challenges that's raising in recent past –



Key Recommendations for Organisations

- Invest in AI-driven security tools:** Leverage the power of AI to automate threat detection, response, and predictive analytics, while staying informed about adversarial AI techniques.
- Prioritise Secure-by-Design Principles:** Integrate security into the development and deployment of IoT and OT devices, ensuring robust authentication, encryption, and update mechanisms.
- Strengthen identity management:** Adopt zero trust principles, implement multi-factor authentication, and monitor for identity-based threats using advanced analytics.
- Secure the expanding attack surface:** Conduct regular risk assessments of IoT, OT, and supply chain environments, and collaborate with partners to address shared vulnerabilities.
- Enhance Supply Chain Security:** Conduct rigorous vetting of suppliers, enforce contractual security standards, and monitor third-party risks continuously.
- Monitor regulatory developments:** Stay abreast of evolving data protection and cyber security regulations to ensure compliance and best practice adoption.
- Foster a culture of cyber resilience:** Provide ongoing security awareness training, develop incident response plans, and encourage collaboration across business units.
- Implement Zero Trust Architecture:** Assume that no device or user is inherently trustworthy, and continuously verify access at every stage.
- Develop Incident Response Plans:** Establish comprehensive procedures for detecting, responding to, and recovering from cyber-physical attacks, with an emphasis on cross-functional collaboration.
- Simulated Exercises:** Conduct drills and simulations to test awareness and readiness for regulatory-driven scenarios, such as data breach notification.
- Training and Awareness:** Run focused campaigns on emerging threats (e.g., phishing, ransomware) and regulatory updates, using posters, emails, and intranet resources.

The expanding digital attack surface presents a difficult challenge for cyber-security professionals and IT leaders. The rapid adoption

of AI, IoT, OT, and smart infrastructure, coupled with emerging technologies like quantum computing and 5G, demands a proactive and holistic approach to risk management. By strengthening security across supply chains, critical infrastructure, and cyber-physical systems, organisations can safeguard their operations and mitigate the real-world impacts of digital attacks. The urgency to act has never been greater; those who anticipate and address these risks will be best positioned to thrive in the hyper-connected world of 2026 and beyond.

Conclusion

The year 2026 promises to be the moment of evolution in cyber security space trying to adapt and managing emerging risks and

growing in digital transformation. The digital environment in which organisations operate is undergoing transformative shifts, driven by the convergence of advanced technologies and increasingly resourceful adversaries. To succeed in this dynamic landscape, organisations must adopt forward-thinking strategies that address the challenges of today while anticipating the risks of tomorrow.

By embracing artificial intelligence responsibly, reinforcing identity management, and proactively confronting new and emerging risks, organisations can enhance their resilience and safeguard their digital future. The journey ahead demands vigilance, adaptability, and a commitment to continuous improvement.

AIMA - Upcoming Events

CAPACITY BUILDING WORKSHOP ON CASE TEACHING & WRITING

08, 09 & 10 January 2026
New Delhi

Topic : Capacity Building Workshop on Case Teaching & Writing
Date : 08th January 2026
Venue: New Delhi



Topic : AIMA's LeadHERship Retreat
Date : 15th January 2026
Venue: Hotel Radisson Blu Palace Resort, Udaipur



Topic : AIMA CSR & Innovation Contest & Summit
Date : 27th January 2026
Venue: AIMA, New Delhi



- 1. South Africa
- 2. Breach Candy, Mumbai
- 3. Udemy
- 4. Urban Company, Snabbit, and Pronto
- 5. Sil
- 6. Cigarettes and Other Tobacco Products Act
- 7. Men's Personal Care
- 8. Udhaiyams Agro Foods