Artificial Intelligence & Cyber Attacks

Emerging Developments, Enhanced Controls & Expanding Capacities

CA. (Dr.) Srinivas Yanamandra

58th Regional Conference of SIRC of ICAI

August 7, 2026

Brief Profile

- **Qualifications**
  - Chartered Accountant from ICAI (2001)
  - Cost Accountant from ICWAI (2000)
  - Doctor of Business Administration (DBA) from Manchester University UK (2013)
- **25 Years of Regulatory Compliance expertise (Banks / Fintech)**
  - Indian Banks - ICICI Bank (2003-14), IDFC First Bank (2015-16)
  - International - BRICS New Development Bank (Shanghai, China) (2017-22)
  - Fintech - Paytm (2022-25)
- **Professional Highlights**
  - TEDx Speaker (2020 / 2023) / Winner of CA Global Achiever Award from ICAI (2019)
  - Visiting Fellow - Cambridge Institute for Sustainability Leadership (2019)
  - Chevening India Cyber Security Fellow - Cranfield University, UK (2025)
- **Academic Engagements**
  - Guest Faculty - Indian School of Business, Hyderabad (since 2020)
  - Non-Resident Senior Fellow - Dhirubhai Ambani School of Law (since 2025)
  - Visiting Professor of Practice - IDRBT (since 2025)

Agenda

Background & Context

AI & Cyber Attack Landscape

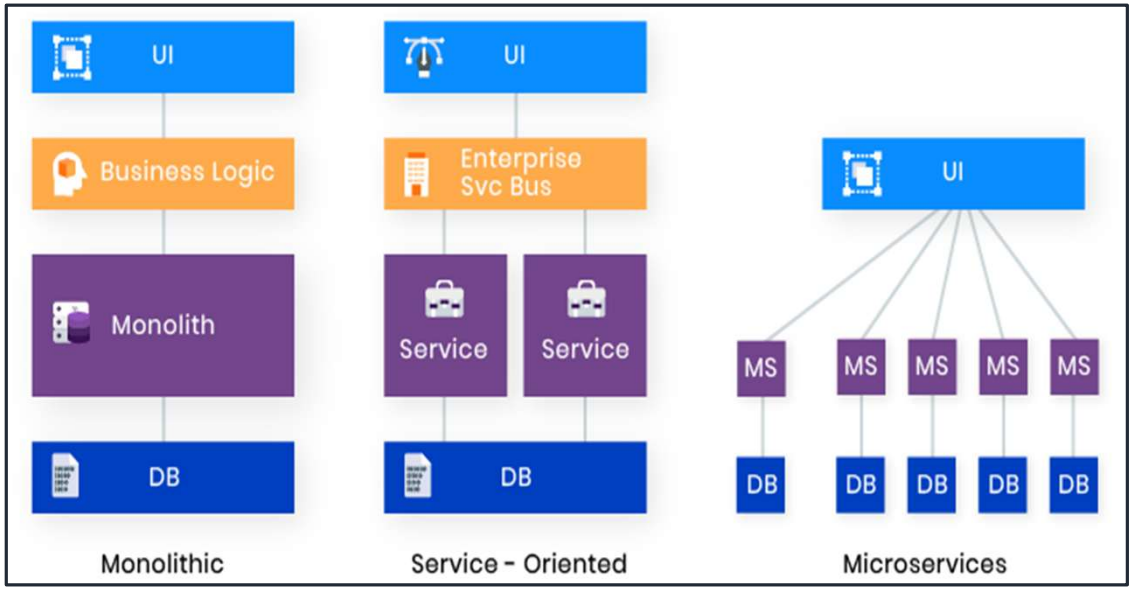
Next Generation Challenges

Capacity Building for CAs

Conclusion

IT Transformation: *From Applications to Architecture*

IT environments evolved from application management to architecture re-design



Food for Workshop Discussion !!!

Transforming banking through:

- APIs - Micro-Service
- APPs - Mobile-First
- APKs - Machine-Code

AI-enabled IT architecture not only results in open-banking, but also enhances cyber attack threat surface

Agenda

- Background & Context
- **AI & Cyber Attack Landscape**
- Next Generation Challenges
- Capacity Building for CAs
- Conclusion

AI-Targeted Threat Surface

Cyber Attackers approach the threat surface with novel uses of AI



Food for Classroom Discussion !!!

Continuous regulatory warnings

- AI-Leveraged Content
- AI-Human Deep Fakes
- AI-Manipulated Models

Current defence mechanisms to guard against external threats insufficient to deal with new age threats

AI-Accelerated Cyber Attacks

Cyber Attacks have increased in sophistication with advancements in AI



Food for Classroom Discussion !!!

Concerning industry updates

- AI-Assisted (Mythos)
- AI-Powered (DeepLocker)
- AI-Initiated (OpenAI)

Coupled with Vibe-Coding, AI-Accelerated Cyber Attacks present a new cyber security challenge

AI-Centric Defense Controls

Cyber Defensive and Offensive operations further being sharpened using AI



Food for Classroom Discussion !!!

Consequent security posturing

- AI-Simulated Defense (VAPT)
- AI-Behavior Analytics (SIEM)
- AI-Directed Response (SOAR)

Current defence mechanisms to guard against external threats insufficient to deal with new age threats

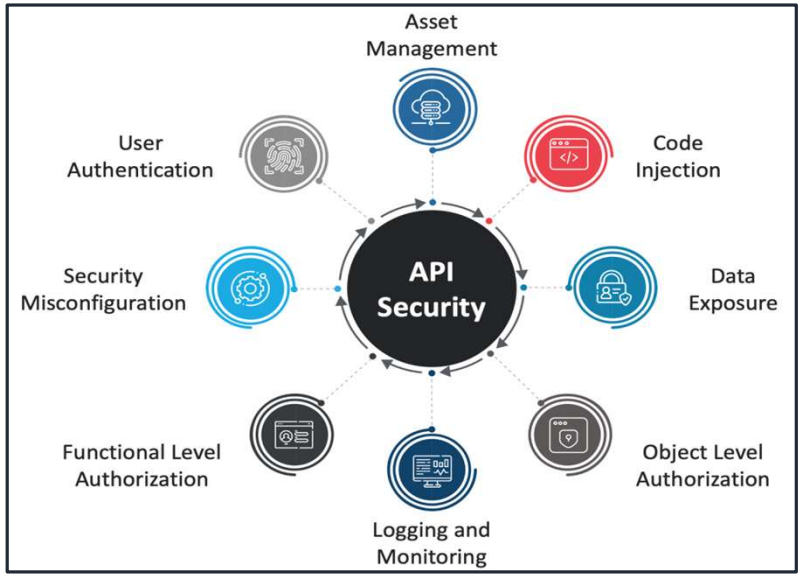
Agenda

- Background & Context
- AI & Cyber Attack Landscape
- **Next Generation Challenges**
- Capacity Building for CAs
- Conclusion

Emerging API Vulnerabilities

How are API risks handled in the organization?

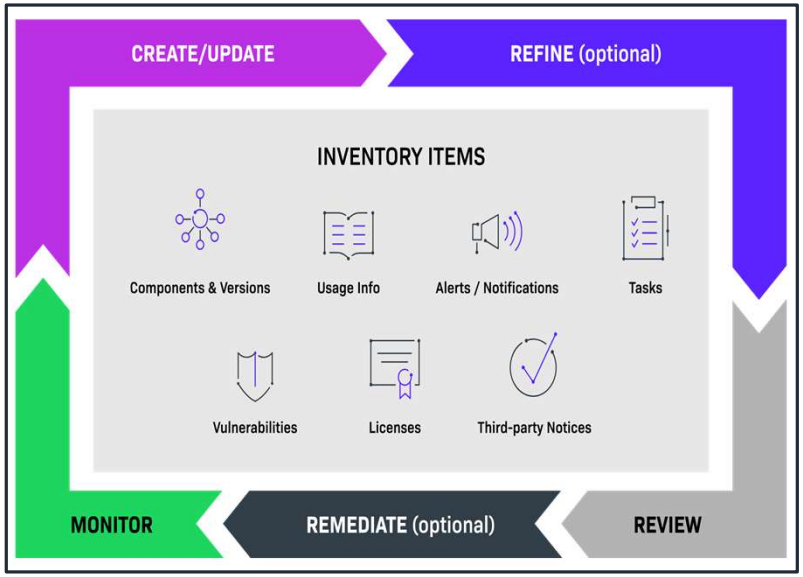
- Finding balance between agility & vulnerability
- Accounting for API inventory
- Formalizing the API due diligence process
- Instituting API controls (e.g., Throttles)
- Case-in-point: *RBI Guidelines on PAs*



Evolving Third-Party Risks

How is supply-chain risk influencing CyberSec risks and mitigation strategies?

- Software Bill of Materials (S-BOM)
- Hardware Bill of Materials (H-BOM)
- AI Bill of Materials (AI-BOM)
- Quantum Bill of Materials (Q-BOM)
- Case-in-point: *CERT-IN Regulations*



Embracing Post-Quantum Challenges

How are cyber risks assessed from PQC standpoint?

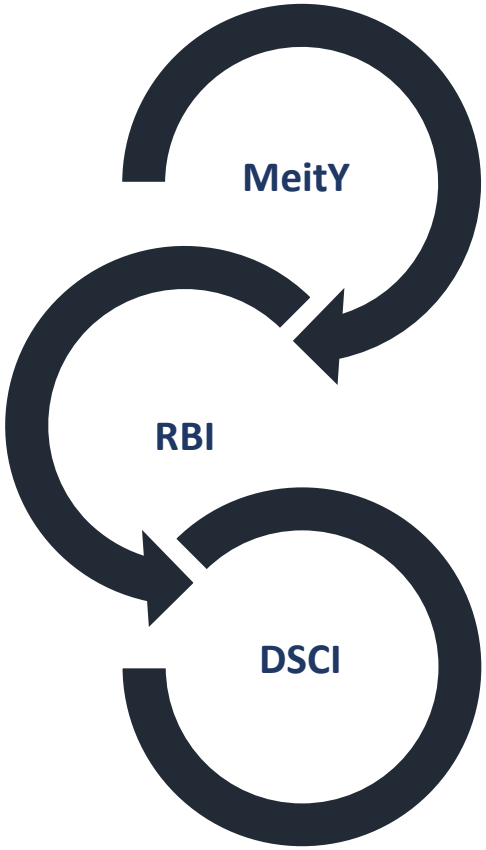
- Current classical computing (KEM / DSA) (S / AS)
- Quantum Threat Horizon (RSA / ECC)
- Paths to PQC - Physics (QKD) / Maths (non-QKD)
- CARAF (existing IT) & Rapid Swap-Out (future IT)
- Case-in-point: *SEBI CSCRF Guidelines*



Agenda

- Background & Context
- AI & Cyber Attack Landscape
- Next Generation Challenges
- **Capacity Building for CAs**
- Conclusion

Follow recent notifications from the Authorities



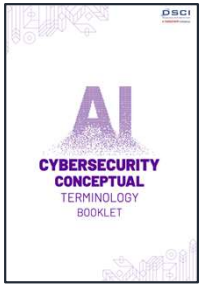
India AI Governance Guidelines - Nov 2025
(*Framework for enabling safe and trusted AI innovation*)



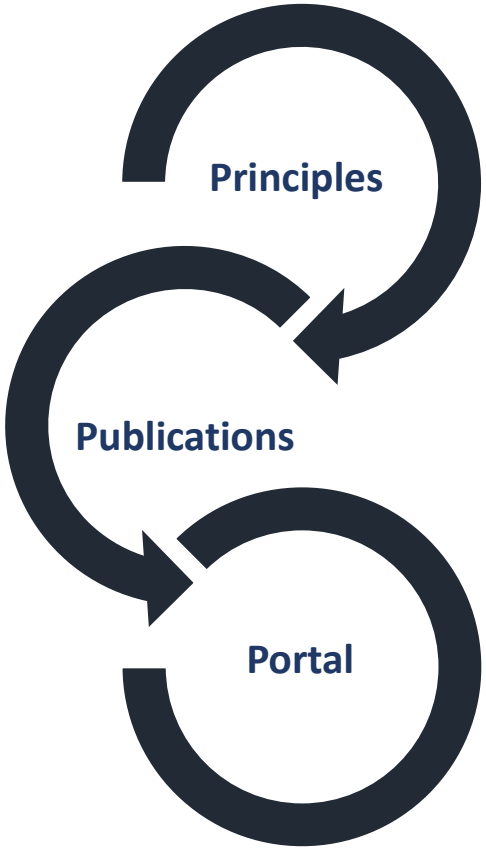
RBI FREE-AI Committee Report - Aug 2025
(*Guidelines on AI-Security / Data Governance / Model Risk*)



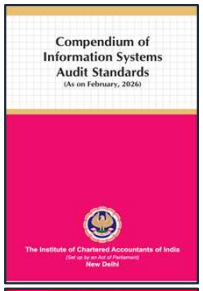
AI Conceptual Terminology Booklet - Feb 2026
(*Reference guide for evolving AI & Cybersecurity terminology*)



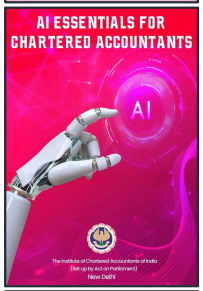
Leverage recent initiatives from the Institute



Compendium of Information Security Audit Standards
(*With comprehensive principle-based framework*)



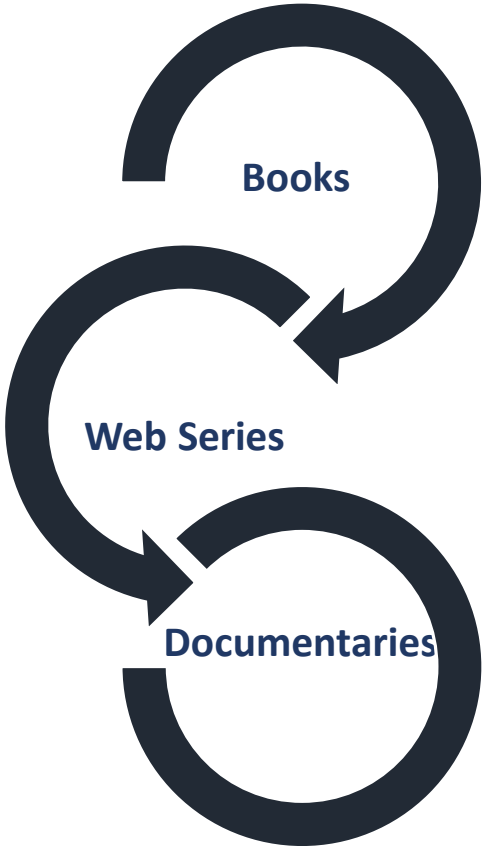
Collection of Publications on AI and Cyber Security
(*With focus on data governance and security aspects of AI*)



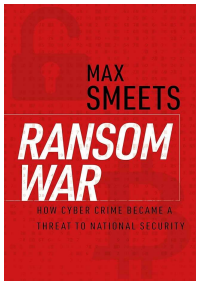
Contemporary initiative to encourage AI expertise
(*With AICA - Level 1 Certification Course for members*)



Convert binge time into learning experience



Journalistic books on cybersecurity investigations
(*Ransom War by Max Smeet - Exploration of Conti Group*)



Dramatized web series on cybersecurity incidents
(*Tehran - A peek into third-party risk management*)



Focused explanation of cyber security concepts
(*Most Wanted Teen Hacker - Biography of Julius Kivimäki*)



Agenda

- Background & Context
- AI & Cyber Attack Landscape
- Next Generation Challenges
- Capacity Building for CAs
- **Conclusion**

Conclusion

AI and Cyber Security		
AI-Targeted Threats	AI-Accelerated Attacks	AI-Centric Controls

Next Generation Challenges		
API	BOM	PQC

Capacity Building for CAs		
RBI	ICAI	Netflix ☺

Thank You

Stay connected:

dryanamandra@icloud.com

+91 98215 09192