SAEIC | South Asian Enterprise & Impact Centre

PEOPLE | IDEAS | SOLUTIONS | IMPACT

KNOWLEDGE
COLLABORATION
RESILIENCE
A STRONGER SOUTH ASIA



Corporate Intelligence & Security

Strengthening Organizational Resilience in a Complex Risk Landscape

ANTICIPATE
PREVENT
PROTECT
RESPOND
EMERGE STRONGER

AN EXCLUSIVE EXECUTIVE WORKSHOP
FOR SENIOR CORPORATE & INDUSTRIAL LEADERS

In a world where threats no longer announce themselves at the gate, the most dangerous vulnerabilities are the ones that go unrecognized – hidden inside systems, people, and processes that organizations trust most.

Today's corporate and industrial leaders operate in an environment where cyber intrusions, insider threats, geopolitical disruptions, ideological infiltration, and industrial espionage are not distant possibilities, they are present realities. The question is no longer whether your organisation will face a security challenge. The question is whether your leadership will be prepared to recognize it, contain it, and emerge stronger.

SAEIC brings together India's foremost security intelligence practitioners, former officials from national security establishments, and corporate risk management specialists, to deliver a learning experience of the highest professional calibre.

Complex Threats. Strategic Leaders. A More Secure Tomorrow.

PEOPLE
INSTITUTIONS
INDUSTRIES
SOCIETIES

ABOUT THE WORKSHOP

FORMAT
Intensive Indoor Executive Workshop

DURATION
3 Days

MODE
Expert-led with case studies, discussions & workshop

VENUE
South Asian University

WHY NOW?

India's corporate and industrial landscape is undergoing a seismic shift. The convergence of digital transformation, geopolitical realignment, and ideological subversion has created a threat environment that most organisations are structurally unprepared to handle.

A MORE COMPLEX WORLD.
GREATER RISKS.



Rising Cyber Attacks

Cyber attacks on Indian enterprises have surged dramatically, with critical infrastructure and manufacturing among the most targeted sectors.

Insider Threats

Insider threats account for the majority of significant data breaches, most originating from trusted employees, contractors, and third-party vendors.

Rogue Actors & Infiltration

Rogue NGOs and ideologically motivated actors are actively penetrating CSR funding channels, labour movements, and regulatory processes within industrial settings.

Accessible Espionage Tools

Open-source intelligence tools have made corporate espionage accessible to low-resource adversaries, turning every digital footprint into a potential attack surface.



ANTICIPATE
PREVENT
PROTECT
RESPOND
EMERGE STRONGER

Conventional security training is no longer sufficient. What is required is **intelligence-led security thinking** at every level of leadership.

WHAT THE WORKSHOP COVERS

This workshop is designed as an immersive, expert-driven engagement. The programme draws from a rich body of subjects spanning the full spectrum of corporate intelligence and security, including:



INSIGHTS
STRATEGIES
CAPABILITIES
REAL-WORLD PERSPECTIVES

01 The Threat Landscape

Understanding the global and national security environment as it directly bears on corporate and industrial operations, state-sponsored threats, external intelligence operations targeting Indian industry, and internal vulnerabilities.



02 Corporate Intelligence & Conceptual Framework

The intelligence cycle, open-source intelligence (OSINT), basics of intelligence collection and analysis, and how intelligence thinking transforms the quality of executive decision-making.



03 Counterintelligence & Information Security

Protecting trade secrets, neutralizing surveillance, securing digital infrastructure, managing social media exposure, and building a counterintelligence posture that is proportionate and legally sound.



04 Protective Security & Access Control

Securing senior leadership and sensitive assignments, access control frameworks, character and antecedent verification of contractual workers, and the application of behavioural science to identify suspicious activity.



05 Crisis Management & Negotiation

De-escalation frameworks, managing mass protests and social disruptions, conflict resolution under pressure, negotiation strategy, and communication management during live security incidents.



06 People, Culture & Institutional Resilience

Gender sensitization and legal compliance, anger and stress management for high-responsibility roles, and building a workplace culture where security awareness is institutional rather than incidental.



07 Industrial Security & Audit

Comprehensive security audit frameworks, threat identification for corporate assets, area survey methodology, and the standards that govern industrial security at the highest level.



WHO SHOULD ATTEND

This workshop is specifically conceived for professionals and emerging leaders from across sectors who are involved in or aspire to work in the domain of corporate and industrial security.



Chief Security Officers & Corporate Security Managers
Enhance strategy, oversight and risk management skills.

Chief Risk Officers & Compliance Heads
Strengthen governance, compliance and resilience frameworks.

Industrial Operations & Plant Heads
Address on-ground security and operational risks.

HR Directors & Administration Heads
Build safer workplaces and manage people-related risks.

IR & Corporate Security Leadership
Navigate industrial relations, threats and crisis management.

IT & Cyber Security Leaders
Understand emerging cyber threats and digital risks.

Legal Vigilance & Audit Officers
Strengthen compliance and monitoring mechanisms.

Senior Executives Involved in Strategic Planning
Align security with long-term business goals.

VIP Protection & Facility Security Personnel
Build practical skills for high-risk environments.

FACULTY

This workshop is led by a distinguished panel drawn from:

- Former Senior Officials of Indian Security Agencies
- Retired Senior Police & Paramilitary Officers from Indian security and counterterrorism
- Corporate Risk Management Consultants with cross-sector deployment experience
- Cybersecurity and OSINT Specialists with national-level mandates
- Legal & Compliance Advisors specializing in corporate law and regulatory frameworks
- Behavioural Scientists with corporate investigation experience

Our faculty brings decades of **real-world experience, operational exposure** and **strategic insight** to ensure a high-impact learning experience.

EXPERIENCE
INSIGHT
IMPACT

FEATURED FACULTY

EXPERIENCE.
PERSPECTIVE.
REAL-WORLD INSIGHT.

Shri Kishor K Sharma

A former senior IB officer and former S.P. UN Police (35+ years) with extensive field experience across Kashmir, Arunachal Pradesh/Assam, Rajasthan, Delhi and the UN Peacekeeping Mission in Cyprus. He is an expert in counter-terrorism, counter-radicalization, counter intelligence, conflict resolution, negotiation skills and industrial security audits.

A post-graduate in Commerce, Labour Laws & Personnel Management, he holds an Honorary Ph.D. in Counter-Terrorism Strategies. He is a recipient of the President's Police Medal for distinguished service, UN Medal and Union Home Minister's Medal for exceptional field operations.

Dr. LMS Ray

A former Senior IB Officer with more than three decades of rich experience in intelligence operations, strategic planning, and training, holds an MBA and Ph.D. in Management.

He has expertise and exposure to varied intelligence skill sets essential for preserving and protecting national security, including specialization in industrial security and Chemical Biological Radiological & Nuclear threats (CBRN).

His career reflects dedication, discipline and excellence in handling operational responsibilities in highly demanding and sensitive environments. He is a recipient of the Indian Police Medal (IPM) for meritorious service.

> All faculty bring not just academic experties, but **field-tested operational knowledge** that no textbook can replicate.

WHAT PARTICIPANTS TAKE HOME

PRACTICAL KNOWLEDGE.
STRONGER DECISIONS.
GREATER RESILIENCE.

01 **Holistic Understanding**
A comprehensive view of the modern corporate threat landscape.

02 **Ready-to-Deploy Frameworks**
Threat intelligence frameworks tailored to their sector.

03 **Practical Tools**
Tools for identifying and managing insider threats, ideological subversion, and physical security risks.

04 **Legal & Ethical Clarity**
A clear understanding of the legal and ethical boundaries of corporate security operations.

05 **Custom Templates**
Ready-to-use templates, checklists and frameworks for immediate use.

06 **Leadership Confidence**
The confidence to lead, not just react, when a security crisis occurs.

ABOUT SAEIC

REGIONAL KNOWLEDGE. REAL IMPACT.

South Asian Enterprise & Impact Centre (SAEIC) was established by South Asian University, following the approval of the competent authority. The Centre functions as its dedicated vehicle for applied research, problem-solving projects, and executive education.

SAU is a university established by the South Asian Association for Regional Cooperation (SAARC), serving Afghanistan, Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan, and Sri Lanka. SAEIC extends that regional mandate into the domain of management scholarship and practice.

CONTACT & REGISTRATION

South Asian Enterprise & Impact Centre (SAEIC)

EMAIL
saeic@sau.int

WEBSITE
South Asia Enterprise Impact Centre (SAEIC) – South Asian University

ADDRESS
South Asian University, Gaushala Rd, Maidan Garhi, New Delhi, Delhi 110068

"Security is not a department. It is a leadership discipline."