HKCS FOUNDATION
Centre for Cyber Excellence...

FEBRUARY

HKIT
CYBER SECURITY EXCELLENCE

NEWSLETTER

Welcome to the HKIT Cybersecurity Newsletter

In today's rapidly evolving digital environment, cybersecurity has become a critical priority for organizations across all industries. The HKIT Newsletter aims to provide valuable insights into the latest cybersecurity trends, emerging threats, security best practices, and industry updates. Through this publication, we share our expertise and knowledge to help organizations strengthen their security posture and stay protected against modern cyber threats.

In This Edition

- Latest Cybersecurity Threat Landscape
- Cybersecurity Tips & Best Practices
- Compliance and Regulatory Updates
- HKIT News and Achievements

Latest Cybersecurity Threat Landscape

Rise of AI-Powered Cyber Attacks

Cybercriminals are increasingly using Artificial Intelligence (AI) to automate phishing campaigns, create realistic deepfake content, and generate advanced malware. AI tools are enabling attackers to launch faster and more targeted attacks against organizations.

Ransomware Attacks Continue to Grow

Ransomware remains one of the most damaging cyber threats, with attackers exploiting unpatched systems and weak credentials to gain access to networks and encrypt critical data. Recent incidents show attackers targeting organizations across multiple sectors.

Botnet and IoT Malware Campaigns

Security researchers recently identified botnet malware exploiting router vulnerabilities to create large networks of compromised devices used for cyber attacks such as DDoS and credential theft.

Advanced Malware & Espionage Campaigns

New malware strains such as GridTide and AI-driven mobile malware are targeting government and telecom sectors, enabling attackers to conduct espionage and steal sensitive data.

Sophisticated Phishing Techniques

Attackers are now using OAuth abuse and advanced social engineering techniques to bypass traditional email security controls and steal login credentials from users.

Cybersecurity Tips & Best Practices

🔐 Enable Multi-Factor Authentication (MFA)

Implement MFA for all critical systems and applications to add an additional layer of security beyond passwords.

🔑 Use Strong Password Policies

Ensure employees use complex passwords and change them periodically. Avoid password reuse across multiple systems.

📧 Beware of Phishing Emails

Employees should verify suspicious emails, links, or attachments before clicking to avoid phishing attacks.

🔄 Regularly Update Systems & Software

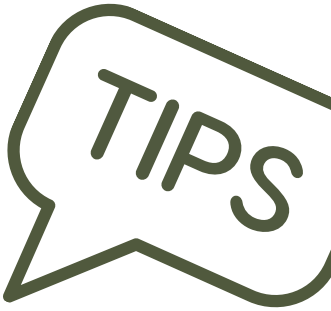
Apply security patches and updates promptly to fix known vulnerabilities in operating systems, applications, and devices.

💾 Maintain Secure Data Backups

Regularly back up critical business data and store backups securely to ensure recovery in case of ransomware or system failure.

👨‍💻 Conduct Security Awareness Training

Train employees regularly on cybersecurity risks, safe browsing habits, and incident reporting procedures.



+91 984 556 8869 info@hkit.in www.hkitsecurity.com

Compliance and Regulatory Updates

Organizations are increasingly required to comply with cybersecurity regulations and standards to protect sensitive data and ensure secure operations. Staying updated with regulatory requirements helps reduce cyber risks and avoid legal penalties.

Strengthening Data Protection Regulations
Governments and regulatory bodies worldwide are introducing stronger data protection frameworks to safeguard personal and sensitive information. Organizations must implement robust security controls and data protection practices.

ISO 27001 Information Security Standard
Many organizations are adopting ISO 27001 to establish an effective Information Security Management System (ISMS). This standard helps organizations manage risks, protect information assets, and improve security governance.

Industry-Specific Compliance Requirements
Sectors such as banking, healthcare, and critical infrastructure must follow strict cybersecurity regulations to protect sensitive data and maintain operational security.

Focus on Third-Party Risk Management
Regulators are emphasizing the need for organizations to assess and monitor the cybersecurity posture of vendors and third-party service providers to prevent supply chain attacks.

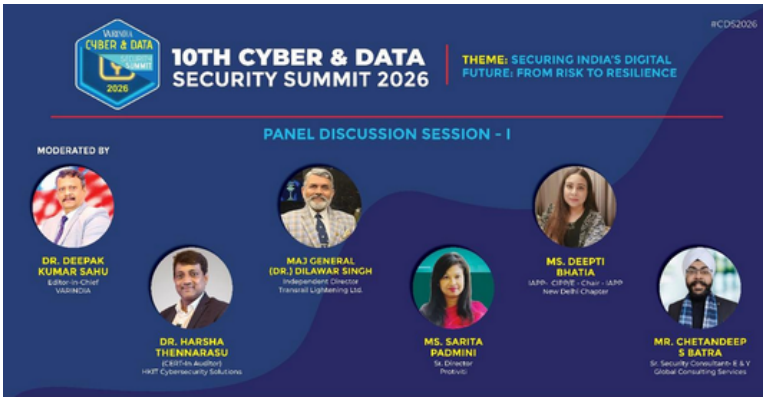
For ISO implementation, certification support, and Data Protection Officer (DPO) consultation services, contact our experts today.

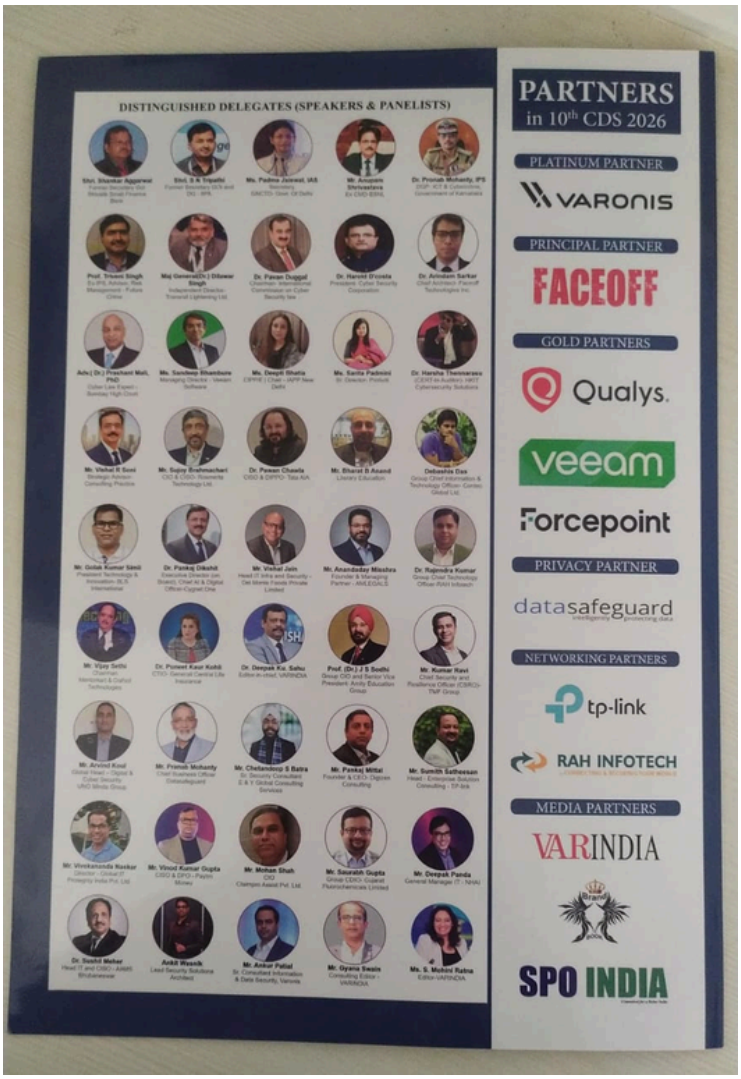
HKIT Achievements – February 2026

Participation in Cyber & Data Security Summit 2026 – New Delhi

In February 2026, HKIT Cybersecurity Solutions marked a significant milestone by actively participating in the Cyber & Data Security Summit 2026 held in New Delhi. Our Director, Dr. Harsha Thennarasu, attended the summit as a distinguished panelist, contributing valuable insights during the panel discussion on emerging cybersecurity challenges and strategies for building a resilient digital future.

The summit brought together leading cybersecurity experts, industry leaders, and technology professionals to discuss evolving cyber threats, data protection frameworks, and the importance of strengthening cybersecurity infrastructure across organizations.





HKIT Achievements – February 2026

Team Building & Skill Development Activities

During the same period, HKIT also organized engaging team-building activities aimed at enhancing collaboration, creativity, and problem-solving skills among employees. The activities included:

- Logical thinking challenges to improve analytical and decision-making skills
- Blindfold drawing exercises designed to strengthen communication and trust within teams
- Mind-stimulating games and activities to encourage innovative thinking and teamwork

These initiatives reflect HKIT's commitment not only to cybersecurity excellence but also to building a strong, collaborative, and innovative team culture.