



10
CPE POINTS

CYBERSECURITY & DATA PRIVACY: THE FIGHT AGAINST FINANCIAL CRIME

29 OCTOBER 2024 | 9.00AM-5.00PM



MyCoID:765264K

HRD CORP REGISTERED COURSE
PROGRAMME NO: 10001454154

PROGRAMME OVERVIEW

The recent catastrophic IT outage sent shockwaves through the global business community, disrupting major sectors of the economy. Travelers were stranded at airports, patients were left waiting in hospitals, and customers found themselves cash-strapped in front of banks. Affecting millions worldwide, this incident starkly underscores the vulnerabilities in our digital infrastructure.

Highlighting the cybersecurity vulnerabilities in our increasingly interconnected digital landscape and the potential for exploitation by cybercriminals, this programme focuses on addressing accountability, rebuilding digital trust, ensuring data privacy, enhancing communication, strengthening operational resilience, and addressing regulatory concerns to ensure businesses' long-term sustainability and security.

PROGRAMME OBJECTIVE

This programme aims to provide insights into the critical cybersecurity vulnerabilities exposed by recent IT outages and other digital disruptions; evaluating the lessons learned from such incidents and implement strategic measures to prevent future occurrences.

ICF COMPETENCY LEVEL

- Core – Risk Management (Proficiency Level 3)
- Functional (Technical) – Digital Technology Application (Proficiency Level 3)
- Foundational (Regulatory) - Capital Market Products Regulation (Proficiency Level 3)

TARGET AUDIENCE

Individuals

Cyber Security Officers, Cyber Security Analysts, Cyber Crime Investigators, Information System Officers, Network Engineers, Digital and Innovation Officers, System Analysts, Professional Hackers, Compliance Officers, Legal Officers, Internal Auditors

Institutions

Capital Market Intermediaries, Public Listed Companies (PLCs), Government-Linked Investment Companies (GLICs), Regulatory and Supervisory Bodies who are keen to learn on cybersecurity and data privacy

WHAT WILL YOU LEARN?

By the end of this programme, participants will be able to:

- recognise the emerging trends in cybersecurity and its potential benefits and threats to business organisations
- assess the impact of IT outages and lessons learned to ensure businesses' long-term sustainability and security
- apply strategies in managing data privacy and cybersecurity risks for resilience and business continuity
- develop strategies to enhance cybersecurity agility and governance by aligning cybersecurity frameworks with organisational goals

PROGRAMME OUTLINE

- 9.00 am **Latest Cyber Landscape and the Future in Cybersecurity**
 - Rise of "zero-trust" security model
 - Emergence of cyberwarfare from Russia-Ukrainian war
 - Gaza conflict: Rise of misinformation and disinformation
 - Adoption of third-party vendors
 - The rise of quantum computing and its impact on security
 - The growth of cybersecurity insurance
 - Cloud security and the metaverse
 - Role of AI and Machine Learning in cybersecurity
- 10.30 am Coffee Break
- 10.45 am **IT Outages Unveiled: Impact, Response, and Resilience Strategies**
 - The ripple effects and risks of IT outages
 - Incident response: Strategies for managing unforeseen downtime
 - Impact on businesses: Operational disruptions, financial consequences, and reputational damage
 - Recovery and resilience: Best practices post-technology outages
 - Discussions on real-life IT outages: Lessons in rebuilding digital trust, enhancing communication, and strengthening resilience for long-term security
- 1.00 pm Lunch Break
- 2.00 pm **Mitigating Risks in Data Privacy and Cybersecurity**
 - Vulnerability in the digital age: Assessing organisational cyber resilience
 - Safeguarding data integrity during system failures
 - Crisis communication: Response plan, stakeholders management and media response
 - Futureproofing for business continuity:
 - Leveraging redundancy and backup systems to prevent catastrophic failures
 - Enhancing infrastructure to mitigate the risk of outage
- 3.30 pm Coffee Break
- 3.45 pm **Leading Cybersecurity Agility and Governance**
 - The role of leadership in driving cybersecurity governance
 - Strengthening governance frameworks to enhance cybersecurity compliance and meet regulatory requirements
 - Adaptive cybersecurity strategies: Responding to emerging threats in real-time
 - Integrating agility into cyber defense: Balancing speed and security
 - Key components of cyber agility: Continuous monitoring and rapid incident response
- 5.00 pm End of Programme

PRICE: RM1300 (not inclusive SST)

SPEAKER



KRISHNA RAJAGOPAL

Krishna Rajagopal is the CEO of AKATI Security and a leading authority in cybersecurity, with over two decades of experience. He is a member of the ISO WG4 committee and has trained military personnel under the U.S. Military Pacific Command. Krishna has served as an expert witness in numerous high-profile cybercrime cases and has advised various governments and law enforcement agencies on cyber defense strategies. He has also been pivotal in shaping global security frameworks, regularly consulting for organizations worldwide. His contributions have earned him a respected reputation in the international cybersecurity community.

Visit www.sidc.com.my for More SIDC Training Programmes **TODAY !**