STRENGTHENING CYBER RESILIENCE SINGAPORE (1 HR)

DETAILED MODULE LEARNING OBJECTIVES

MODULE	OBJECTIVES & OUTCOMES
Strengthening Cyber Resilience Singapore	At the end of the module, participants will be able to: • Gain an understanding of the new set of rules issued by MAS aimed at raising the cyber security standards and strengthening cyber resilience of Financial Institutions in Singapore. • Understand cyber threats, MAS Notice on Cyber Hygiene, impact to FI's operations, cyber hygiene practices which include administrative accounts, security patches, security standards, network perimeter defense, malware protection and multi-factor authentication, the integration of Cyber Hygiene, Technology Risk Management Guidelines and Business Continuity Management Guidelines, and how cyber security is managed internally. • Be kept abreast of the trends and developments of the relevant laws and regulations aimed at raising the cyber security standards and strengthening cyber resilience relating to their fund management business in Singapore.

TOPICS COVERED IN THE MODULE

1. Cyber Threats
2. Security Challenges in the Financial Industry
3. Rising Costs
4. Phishing
5. Data Theft
6. Malware Attack
7. MAS Notice on Cyber Hygiene
8. Application of Notice
9. Impact on Notice to FI's Operations
10. Cyber Security Measures
11. Administrative Accounts
12. System Vulnerabilities
13. Security Standards
14. Multi-factor Authentication
15. Applicability of Multi-Factor Authentication
16. Technology Risk Management ("TRM")
17. Business Continuity Management ("BCM")
18. Cyber Hygiene Vs TRM
19. How Cybersecurity is managed internally?
20. Collective Prevention of Cyber Threats