Cybersecurity

PROSPECT

PROSPECT ACADEMY

PRINCIPLES OF CYBERSECURITY FOR EMPLOYEES

Empower Your Digital Responsibility

WHAT'S IN IT FOR ME?

Every employee, from entry-level to executive, plays a pivotal role in safeguarding their organization. Through this training, you will be prepared to actively contribute to your organization's cyber defence strategy, enhancing both your personal security acumen and the collective resilience of your workplace.

You Will Learn:

- Why is the need of cybersecurity and data privacy?
- What are the basic concepts and terms of security?
- What do I need to know about security risk and the basic controls?
- Why do we need security principles and what are they?
- What are the technical components of security?
- How to ensure secrecy of data and messages?
- How do we assert who requires access to secure data?
- What to do when a security breach occurs?

COURSE OVERVIEW

This **Two-days** cybersecurity fundamentals course is designed to give participants a foundational understanding of cybersecurity concepts and principles. Cybersecurity is a critical area of concern for individuals, businesses, and organizations alike, as cyber-attacks and data breaches can result in significant financial, reputational, and legal consequences. Each individual employee of any organization has his/her contribution of "See something, do something" to strengthen the Cybersecurity posture of the organization. Since, *Security is every one's responsibility.*

COURSE OUTCOMES

After completing this course, YOU/Employee will be able to:

- Appreciate the purpose of Information Security in the organization
- Contribute effectively to the objectives of Information Security in the organization
- Support the Objectives of Information Security in the organization
- Capable of instilling, practicing, and enhancing the Security Hygiene
- Appreciate the Cybersecurity Agency's Cyber-Essential and Cyber-Trustmark standards
- Qualify to appear in the ISO/IEC 27001 Information Security Foundation training
- Qualify to appear in the ISO/IEC 27032 Cybersecurity Foundation training
- Apply the knowledge to prepare for entry-level Professional Certification, CC

COURSE DURATION

Two (2) Days / Sixteen (16) Hours

COURSE FEE

SGD$550.00 (Excluding GST) Prevailing GST rates apply

COURSE OUTLINE

Topic 1 - **Cybersecurity and Privacy Introduction**

- Introduction to Security: Information & Cyber
- Purpose of Cyber Security and Data Privacy
- Why is Cyber Security critical?
- How does Cyber Security and Data Privacy differ
- History of Cyber security and its evolution
- The Statistics and Status of Cyber Attacks

Topic 2 - **Concepts Terminology**

- The Security TRIAD and DAD
- The key concepts of Security
- The fundamentals of Security
- Layered Security principle
- From Assets to Attacks

Topic 3 - **Security Risk, Policy, and Controls**

- Cyber Security Policy, Procedures, Standards & Guides
- Cyber Threats. Vulnerabilities, and Risk
- Cyber Audit and Compliance
- Control Safeguards and Countermeasures

Topic 4 - **Security Principles & Primaries**

- The 5 Cyber Security principles: Governance, Protect, Detect, Response, and Recover
- The 7 Privacy principles: General, Notice and Choice, Disclosure, Security, Retention, Data Integrity, Access Principle
- The Key Threats, Vulnerabilities, Attacks and Controls

Topic 5 - **Security Elements**

- 5 key security elements: Network, Information, Application, Operational, and End-user
- Staying Secure While in the Office

Topic 6 - **Cryptography**

- Basics of Information secrecy and concealment
- Objective of Cryptography

Topic 7 - **Identity and Access Management**

- IAAA Concepts
- Authentication: purpose and multi-Factors of Authentication

Topic 8 - **Incident Response**

- Purpose and definition of Security Incidents
- Incident Stages

COURSE OBJECTIVES

It covers key topics such as cybersecurity terminology, security controls, identity and access management, cryptography, and incident response. The course aims to equip participants with the knowledge to understand and communicate about cybersecurity effectively, implement security controls, manage access to information securely, understand the basics of cryptography, and respond to cybersecurity incidents efficiently. By the end of the course, attendees will be prepared to both apply their knowledge in practical situations and pursue advanced studies in cybersecurity, fostering an environment of continuous learning and adaptation in the face of evolving digital threats.

WHO SHOULD ATTEND?

- Broad Audience: Any employee within any organization, regardless of role
- Information Handlers: Individuals who access any organizational data or digital assets
- Security-Conscious: Those concerned about cyber threats and organizational risks
- Future-Oriented: Employees aiming to enhance their cyber risk management skills

PRE-REQUISITES

- A concern for the protection of your organization against cyber threats
- Your organization has been a victim or a potential a victim of any cyber-crime or scam
- Basic proficiency in reading, writing, and speaking English

NEXT STEPS

This course will assist an attendee to prepare for the Certified in Cybersecurity Certification (CC) Exam from ISC2, the world's largest network of certified cybersecurity professionals entity that helps them continue their professional development and earn new achievements and qualifications throughout their career. The topics on the CC exam included in this 2 hours with100 MCQ exam:

- Security Principles
- Incident Response, Business Continuity (BC) and Disaster Recovery (DR) Concepts
- Access Controls Concepts
- Network Security
- Security Operations

READ NOW

REGISTER NOW

2, Alexandra Rd, #03-01B Delta House,
159919, Singapore
+65 9239 5917
prospectprotection.net