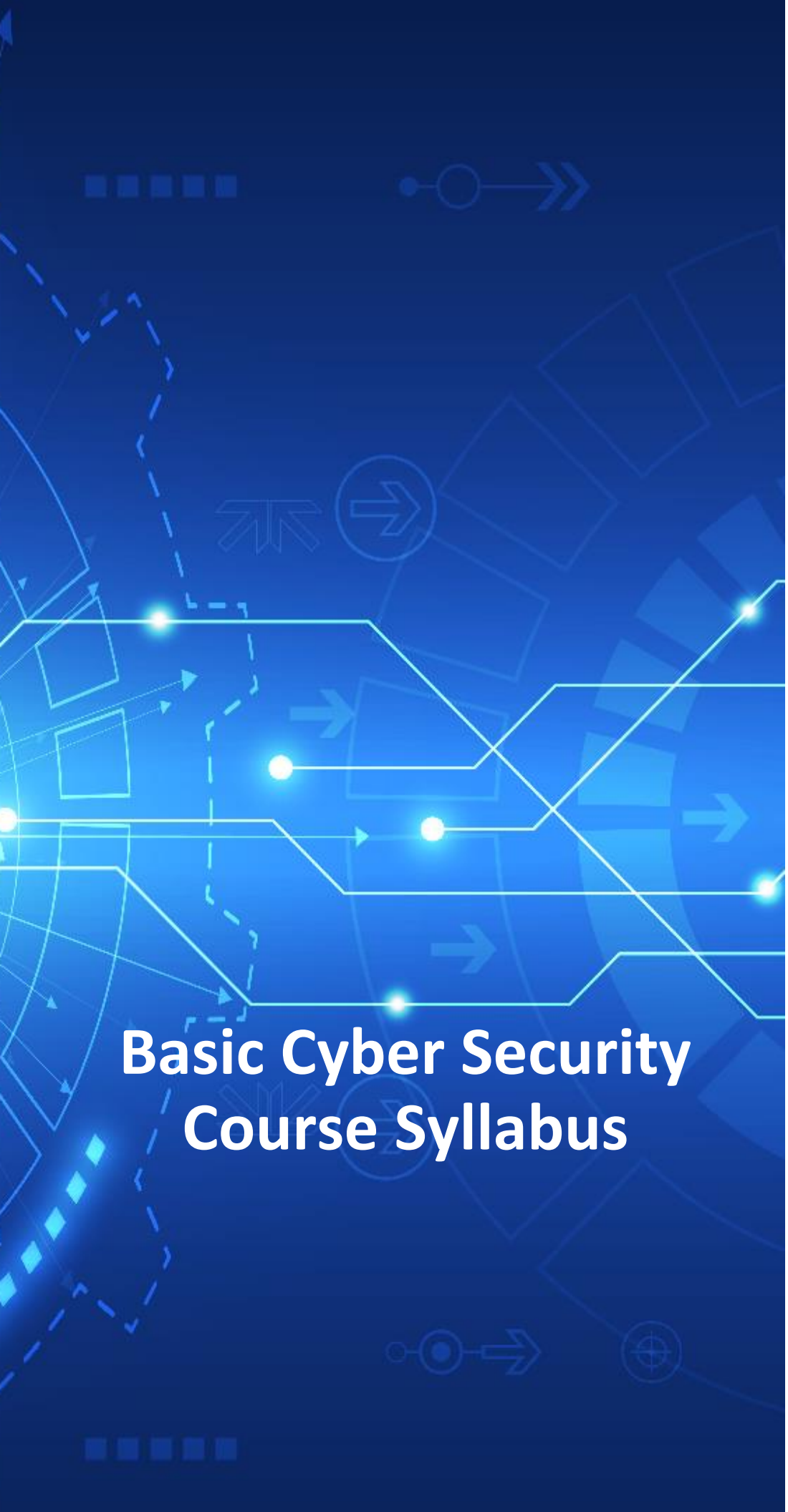

Basic Cyber Security Course Syllabus

C. MER Industries Ltd.
5 Hatzoref St., Holon 5885633, Israel
T+972-3-5572555 F+972-3-5580282
www.mer-group.com | info@mer-group.com

1. Contents

Information Security in a Cyber World Cybercrime and cyber terrorism are a growing threat to organizations of any kind, driven by sophisticated malefactors who are using a variety of technologies and modes of operation.

Cyber threats include:

- Stealing funds and data from the organization
- Selling proprietary data to competitors or other criminals
- Stealing identities of customers, employees or users
- Committing fraud and large-scale attacks

Despite these serious threats, the level of awareness among employees in numerous organizations is low and IT departments lack dedicated training and a security knowledgebase. Professional training is therefore necessary to protect the organization's assets and resources.

Learning by Doing

MER is offering a unique training program to help organizations reinforce their security posture and make sure all employees are aware of the risks and security measures that are required in their roles.

Training is tailored for the specific needs of each organization and includes the following components:

- Developing a specialized training program for the organization
- Lectures and lessons for transferring professional knowledge
- Simulation of cyber-attack for gaining hands-on experience

With over 5,000 Hours in training, we can assure our staff is ready for any task.

2. Basic Cyber Training

2.1 Course Description

The Cybersecurity Fundamentals Course will provide learners with principles of data and technology that frame and define cybersecurity. Learners will gain insight into the importance of cybersecurity and the integral role of cybersecurity professionals. We will explore foundational cybersecurity principles, security architecture, risk management, attacks, incidents, and emerging IT and IS technologies.

- Number of participants: up to 30.
- Number of trainers: 1.
- Length: 4 days.

2.2 Target Audience

- No background students.
- Audit, risk, compliance, information security, government and legal professionals with a familiarity of basic IT concepts who:
    - Are new to cybersecurity.
    - And/or are interested in entering the field of cybersecurity.

2.3 Course Objectives

- Understand Networking
- Understand Communication Between Computers on a network
- Identify OSI Model / TCP /IP model
- Describe Network components
- Identify Protocols
- Distinguish Command Line
- Understand Proxy and VPN
- Understand the Cloud World
- Understand the Internet
- Understand the importance of Cyber Awareness
- Identify and prevent Social Engineering
- Understand the Internet Identities
- Aware to the threats on the smartphones
- Understand DeepWeb and DarkNet
- Aware of Mail Server
- Understand Internet anonymity
- Know Famous attacks
- Understand what is Cyber Security
- Understand basic concepts of Cryptography

2.4 Course Syllabus

- **Introduction to Networking**
    - What is a network? How is it built? Why do we need it? What is LAN & WAN? Network Topologies
- **Communication Between Computers on a network, OSI Model / TCP /IP model - Basic**
    - How computers communicate with each other on the internet
    - MAC address
    - SWITCH
    - TCP / IP
    - ARP
    - ROUTER
    - HTTP
    - UDP
- **Network components - Basic**
    - Proxy VS NAT/ PAT
    - Router vs Switch & Network Devices
- **Command Line - Basic**
    - Understanding the interface, commands and common uses
- **Command Line - Guided Exercise**
    - Practice
- **Protocols**
    - Basic explanation and examples of protocols
- **VPN – Basic**

- **Network security components and concepts – Basic**
    - Firewall
    - IDS / IPS
    - NAC
    - DMZ
    - Gateway Proxy
    - Honey Pot
- **Introduction to the Internet**
    - Internet history
    - Basic concepts, protocols and services
- **Mail Server**
    - Basic protocols, types of mail servers
- **Cloud World - Basic**
    - What is the Cloud
    - Why to work with the Cloud
    - Buy or Rent
- **Intro to Cyber Security**
    - Cyber Crime
    - Cyber Security
    - Inside and External attacks
    - Concepts: hardware, software, data, network, human factor, Trojan, USB, malware, viruses, worms
    - Common types of attacks- low level: email, public internet access, routers, smartphones
    - Hackers
    - Hacktivists
    - Password cracking
    - Examples of real attacks- Carbanak & Stuxnet

- **Internet Identities**
    - Identities and Profiling
- **Cyber Awareness**
    - What is Cybersecurity
    - Man in the Middle
    - Google Hacking
    - SQL Injection
- **Famous Attack Methods**
    - Famous attack methods in a nutshell – DoS & DDoS, Social Engineering, Phishing, Spoofing, Defacement, Password Attacks
    - Social Engineering example.
- **Ransomware**
    - Basic concept, how to be protected, example of famous incidents –Wannacry/PETYA
- **Cellular and Smartphones Security and Threats**
- **DeepWeb and DarkNet**
    - Basic lecture of the concepts, how they formed, what can be found there, their importance to the Internet world, hazards, etc.
- **Internet anonymity**
    - Types of anonymity systems
    - TOR
    - I2P
- **Cryptography**
    - Cryptography building blocks
    - Types of ciphers and authenticators
    - Keys pre distribution process – Asymmetric vs. Symmetric

- SSL - Handshake