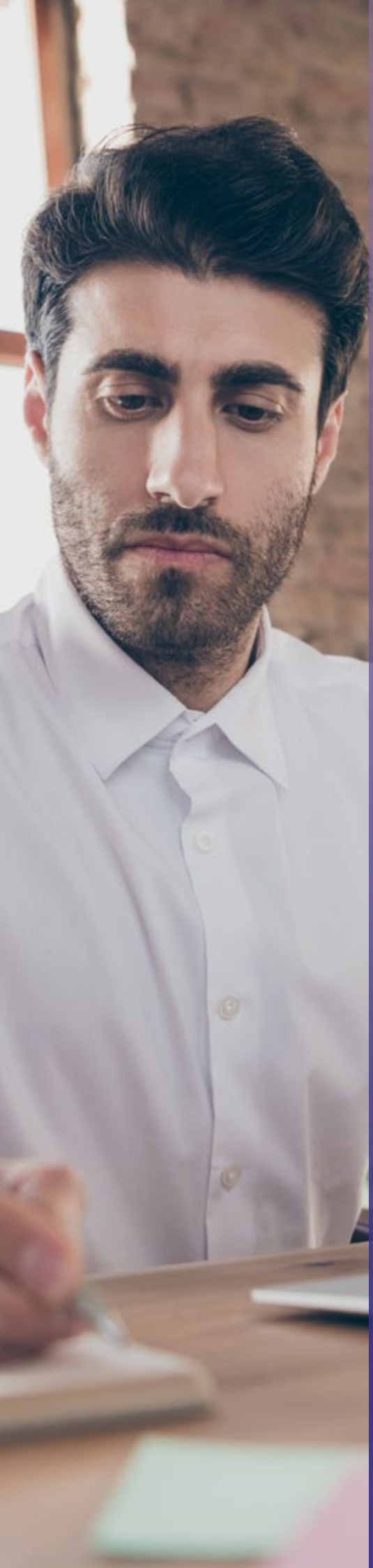

HackerU PRO UPDATE NEEDED

QAI

Cybersecurity Essentials for Executive Management

16
Academic
Hours

Cybersecurity Essentials for Executive Management

Outline

In recent years, cyberattacks have become more sophisticated and dangerous for companies and corporations due to the theft of sensitive data, shutdowns of critical infrastructures, the encryption of essential documents, and more.

The prevailing thought in the cyber world is that the human factor is the weakest link of the cybersecurity chain, so to reduce risks, organizations must offer proper training to raise employee awareness and minimize the risks of security incidents.

During this training course, we will review the cyber challenges experienced by the technical layer of an organization and learn about both internal and external attacks. To understand the process of an attack and minimize threats in the office and home, managers will learn how to define security polices and regulations focusing on the Indian market.

Target Audience

The course is meant for high-level executive managers.

Prerequisites

- Basic computer skills.
- Basic+ knowledge of English.

Objectives

Upon completing this course, delegates will be able to:

- Have a better understanding of current widespread cyber attacks.
- Understand security risks involving personal equipment.
- Understand the risk of unpatched services.
- Efficiently create security policies.
- Improve existing security policies.

Content

Module 01
Overview

- Attack vectors:
  - DNS Spoof
  - DDOS
  - Brute-Force
  - Others

Module 02
Social Engineering Methods and Security Awareness

- Phishing:
  - Email security
  - Suspicious emails or addresses
  - Suspicious file extensions
  - Suspicious links
  - Awareness of phishing emails
- Passwords:
  - Strength and length
  - Never save passwords as cleartext
  - Use password complexity
  - Usage of unique passwords
  - Never use old passwords or the same password for different applications
  - Password security solutions
  - Two-factor importance & methodology
- Personal Equipment - BYOD:
  - Restriction of personal drive usage
  - Restriction of personal laptops
  - Restriction of copies or backups of company information or software

Module 03
Defining Security Policies

- Security Strategy Planning
- Security Policy Scoping
- How to create a backup plan
- How to create a Disaster Recovery Plan
- Creating an organizational security policy
- Compliances & regulations
- How to follow ISO standards

Module 04

Open-Source Intelligence (OSINT)

- The importance of gathering information
- Data types that can expose organizations
- Open-source intelligence terminology & definitions
- Darknet
- Types of OSINT sources:
  - Google dorks for OSINT
  - Maltego (automation)
  - Shodan

Module 05

Risk Assessment & management

- Threat modeling
- Case studies of policy
- Protection control types
- Computer laws and crimes
- Audit and assessment
- Risk management
- Risk evaluation
- Risk response
- Cyber in India – CRT Team Management

raise employee awareness and
minimize the risks of security incidents.