Faysal Aziz

# Course Outline Cybersecurity-1

FA-0461

Cybersecurity

---

## Introduction

There are two types of organizations: those who know they have been hacked and those who don't. Nearly every day there is news about a hacked company, regardless of their size.

The amount of data available today is unprecedented. Along with the advantages that this data provides comes new risks for companies in all industries. One of the most important threats to companies is cybersecurity. A cyberattack can target any part of a company's operations, from customer data to proprietary information, and can have devastating consequences. The importance of cybersecurity cannot be overstated.

Companies must take steps to protect themselves from cyberattacks.

This course walks you through various aspects of cybersecurity and will make you battle-ready to deal with the cyber threats your organization faces.

## Learning Outcome

## By the end of the course the learner would have:

- A deep understanding of the various cyber security standards
- Knowledge to apply the standards
- Understanding to devise cybersecurity strategies and policies
- Get abreast of the modern and evolving cyber threats
- Ability to apply risk and vulnerability assessments
- Knowledge to understand and deploy ISA/IEC 62443 industrial security framework

- And a lot more

# Prerequisites

# Basic understanding of computers and security.

# Duration: 2 days

# Training outline

## 1. Day 1

## 2. Principles of long-term cybersecurity

1. Security policies
2. Security assessment models
3. Monitoring for threats
4. Rapid response policies

## 3. ISA/IEC 62443 industrial security framework

1. What is ISA/IEC 62443?
2. Purpose of ISA/IEC 62443
3. Key concepts of ISA/IEC 62443
4. The ISA/IEC 62443 series details
5. Maturity and Security levels
6. How to apply SA/IEC 62443 to your organization

## 4. Risk and vulnerability analysis

1. What is risk analysis?
2. Different stages of risk analysis
3. Risk analysis techniques
4. Occasions for risk analysis

5. What is vulnerability analysis?
6. Different stages of vulnerability analysis
7. Common vulnerabilities
8. Differences between risk and vulnerability analysis
9. Applying risk and vulnerability analysis to your organization

## 5. Defense in depth or layered security

1. Different layers of security
2. Difference between defense in depth and defense in breadth
3. Characteristics of Defense in depth
4. Adopting layered security / defense in depth

## 6. Day 2

## 7. Zones and Conduits

1. Defining Zones and Conduit
2. How to correctly set up zones and conduit
3. General types of conduits
4. Different levels of segmentation

## 8. Principles behind risk mitigation techniques

1. Risk mitigation strategies
2. Layers of risk mitigation
3. Anti-virus
4. Firewell
5. Virtual Private Network

## 9. Emerging trends in cybersecurity threats

## 10. Case Studies of Security Policies

© 2026 Faysal Aziz · Kuala Lumpur