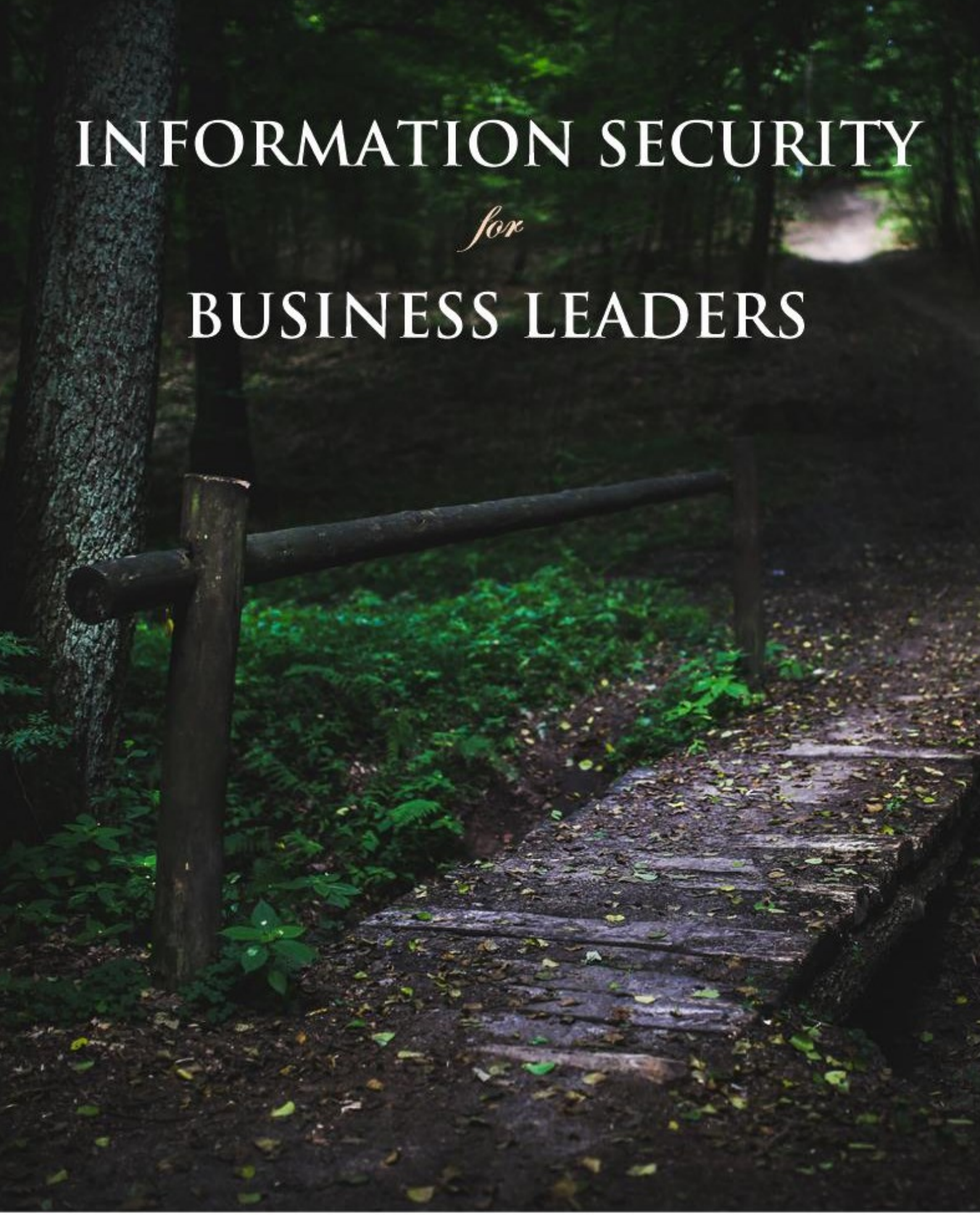
INFORMATION SECURITY

for

BUSINESS LEADERS



Forebrook

INFORMATION SECURITY

Information and information systems are critical to any organisation in this age. Access to reliable information is a business need and information is a valuable asset. Protection of information and information systems then becomes synonymous with protecting the business.

Organisations continue to face increased risk to information assets and systems that store, process and transmit information. Not only has cybercrime increased in volume but also in sophistication. The executive management bears the responsibility for a major portion of the task of protecting information assets and systems. Effective security requires the active involvement of executives to assess emerging threats and the organisation's response.

WHO SHOULD ATTEND

- CIOs, CISOs, IT Heads, IT Managers, Risk Managers, IT Security and Risk Professionals.
- IT Auditors, Audit Managers, Compliance Managers, Regulators, Fraud Examiners.
- Senior Management, IT Strategists.

WORKSHOP PRESENTER

Ahmed S Anwar is a senior information security and governance consultant and trainer, with more than 18 years' experience in information security, systems & networking, governance, risk and compliance. He is certified in governance of enterprise IT (CGEIT) in addition to other certifications such as CISSP, CISA, CISM, CRISC, PMP, C/CISO, MCTS and MCSE. He has previously worked in a federal government organisation in Dubai, where he was the Head of Systems, Networking and Security.

PROGRAMME

8.30 – 9.00	**Arrival**
9.00 – 10.00	**Session One**
10.00 – 11.00	**Session Two**
11.00 – 11.15	**Break**
11.15 – 12.15	**Session Three**
12.15 – 1.15	**Session Four**
1.15 – 1.30	**Closing**
1.30 PM	**Lunch**

KEY LEARNING OBJECTIVES

- Information Security Concepts
- Information Security Related Risks
- Major Data Breaches and Losses
- Security Standards and Frameworks
- The Need for Security Governance
- Commitment of Executive Management for Information Security
- Understand Common Threats
- Information Security and Emerging Technologies and Trends
- Need for Security Assessments
- Role of People in InfoSec

TOPICS

SESSION ONE

Major Security Breaches in Recent Years / Estimated Losses

Some InfoSec Related Statistics

Why Should You Worry About Information Security

What is at Stake?

Who is After Your Data?

Risks of Ignoring Information Security (or Why InfoSec is High-Priority)

State of Information Security Worldwide (Highlights from 2021-22 Surveys & Reports)

SESSION TWO

Introduction to Information Security

Objectives of InfoSec: The C-I-A Triad

Key Concepts: Vulnerabilities and Threats

Key Concepts: Malware and Exploits

Common Attacks and Countermeasures

Security Controls: Management, Operational and Technical Controls

Key Questions You Should Ask Your Security Department

SESSION THREE

How Much Security is “Enough”?

Information Security Strategy

Security Policies

Corporate Governance, IT Governance and Security Governance

Commitment of Executive Management and Ownership of Security

Committing Resources for InfoSec

Integrating Security in Business Processes

Business Continuity / Disaster Recovery

SESSION FOUR

Compliance

Information Security Frameworks and Standards

Quick Overview of ISO27001:2013 and PCI-DSS 3.1

Security Activities

- Monitoring, Incident Handling
- Access Control
- Security Assessments, VAPT
- Physical Security

Security Related IT Investments

- SIEM, Log Management
- Firewalls, Web Firewalls, Next-Generation Firewalls
- Identity and Access Management
- Vulnerability Management System
- IDS/IPS, Anti-Malware, Spam Control
- DLP

Cloud Security

BYOD, Mobile Computing, Social Media and Internet of Things (IoT)

Mobile Payments

Human Factor in Security; User Awareness

WHAT NEXT?

Road Map: Assess – Analyse – Prioritise – Remediate – Continuous Improvement