PDPA & Cybersecurity Practitioner with 72-Hour Breach Response Simulation – Course Outline and Schedule

3 days training

Introduction

In 2026, data protection is a legal mandate. This comprehensive program aligns with the **Personal Data Protection Act (PDPA) 2024 Amendments** and the **Cyber Security Act 2024 (Act 854)**. Over three days, participants move from foundational legal awareness to a hands-on mastery of mandatory breach notifications, ensuring organizations can navigate the critical 72-hour window while minimizing legal and reputational risks.

Learning Objectives

- **Understand** the legal implications of **Act 854** and the mandatory **PDPA breach notification** requirements.
- **Identify and Mitigate** risks of data leaks, ransomware, and AI-driven cyber threats in daily business operations.
- **Apply** a practical framework to conduct internal **Data Protection Impact Assessments (DPIA)** and security audits.
- **Master** the 72-hour countdown by learning to build a **Breach Response Team** and navigate official reporting mechanisms.
- **Demonstrate** commitment to digital ethics and **Social Responsibility (ESG)** by protecting privacy and signing a **Digital Integrity Pledge**.

Target Participants

- **Business Owners & Directors:** To understand personal liability and the new "Direct Responsibility" for data processors.
- **Appointed Data Protection Officers:** Legally mandated to oversee privacy, manage the Breach Register, and communicate with the Commissioner.
- **HR & Administrative Managers:** Professionals handling sensitive employee biometric and payroll data.
- **IT Managers & System Administrators:** Staff responsible for implementing technical safeguards and leading incident escalation.
- **Compliance & Risk Officers:** Individuals tasked with ensuring the company is "Audit Ready" and maintaining internal control mechanisms.

Methodology

The program uses a **Practical Awareness and Simulation Approach**. Days 1 and 2 utilize **Scenario-Based Discussions** and **Real-World Case Studies**. Day 3 transitions into a **72-Hour Breach Drill Simulation**, where participants apply their knowledge in a realistic crisis scenario to produce draft notification reports and response workflows.

© Knowledge Tree PLT
www.cadtraining.com.my

Course Outline and Schedule

Day 1: The Legal Mandate & PDPA 2026 Compliance

Time	Topic / Activity
9.00 a.m. – 9.30 a.m.	**Foundation: Data Privacy & The Regulatory Framework** * Trainer & participant introduction; Expectation setting; Why PDPA and the Cyber Security Act matter in 2026.
9.30 a.m. – 10.30 a.m.	**The New Landscape of Malaysian Law** * Overview of **Act 854** and **PDPA 2024 Amendments**; Legal risks & liabilities for "Associated Persons" and Directors.
10.30 a.m. – 12.15 p.m.	**The Mandatory Data Protection Officer & Audit Readiness** * Who must appoint a DPO?; Duties and personal liability; Registration process with the Commissioner.
12.15 p.m. – 1.15 p.m.	**Lunch Break**
1.15 p.m. – 2.30 p.m.	**Mandatory Breach Notifications** * The 72-hour rule; Documentation and maintaining a Breach Register; When and how to notify the Commissioner.
2.30 p.m. – 3.45 p.m.	**Data Protection Impact Assessments (DPIA)** * Conducting risk audits; Updating privacy notices for 2026 standards; Managing data portability.
3.45 p.m. – 4.30 p.m.	**Internal Reporting & Data Rights** * Overview of internal control mechanisms; Managing individual "Right to be Forgotten" requests; Reporting misconduct basics.
4.30 p.m. – 5.00 p.m.	**Day 1 Summary & Compliance Reflections** * Key legal takeaways; Q&A session; Building a "Privacy-First" mindset.

© Knowledge Tree PLT
www.cadtraining.com.my

Day 2: Cybersecurity Defense & Audit Readiness

Focus: Practical Security Measures to Satisfy the "Security Principle".

Time	Topic / Activity
9.00 a.m. – 10.30 a.m.	**Anatomy of 2026 Cyber Threats** * AI-enhanced phishing, deepfake scams, and ransomware evolution.
10.30 a.m. – 12.15 p.m.	**Technical Safeguards & Access Control** * MFA, Encryption, and "Least Privilege" for satisfying security audits.
12.15 p.m. – 1.15 p.m.	**Lunch Break**
1.15 p.m. – 3.00 p.m.	**Developing an Incident Response Plan (IRP)** * **Workshop:** Drafting a 1-page Emergency Response protocol.
3.00 p.m. – 5.00 p.m.	**Final Audit Preparation & Summary** * Preparing for NACSA/PDPC visits; Building "Cyber Hygiene".

© Knowledge Tree PLT
www.cadtraining.com.my

Day 3: The 72-Hour Breach Response Simulation *Focus: Practical Mastery of the Mandatory Notification Window*.

Time	Topic / Activity
9.00 a.m. – 10.30 a.m.	**Determining "Reportability" & Severity** * Is the breach reportable?; Assessing incident severity and potential "Significant Harm".
10.30 a.m. – 12.15 p.m.	**Activating the Response Team** * Incident escalation; Evidence preservation; Building the 72-hour countdown workflow.
12.15 p.m. – 1.15 p.m.	**Lunch Break**
1.15 p.m. – 3.30 p.m.	**Regulatory & Individual Notification Mastery** * Drafting reports for the Commissioner; Communication strategies to prevent reputational damage.
3.30 p.m. – 5.00 p.m.	**The 72-Hour Breach Drill Simulation** * **Simulation Scenario:** "The Midnight Database Leak"; Delivering breach classifications and notification drafts.

Workshop Deliverables: Participants receive a **PDPA Breach Response Toolkit**, **72-Hour Response Checklist**, and **Breach Classification Decision Tree**.

© Knowledge Tree PLT
www.cadtraining.com.my