MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

RANSOMWARE PREPAREDNESS AUDIT: REVIEWS THE ORGANIZATION\'S READINESS TO PREVENT AND RESPOND TO RANSOMWARE ATTACKS

“Auditing Cyber Resilience and Response Capabilities Against Ransomware Threats”

Schedule

Date	Venue	Fees (Face-to-Face)
11 – 15 May 2026	London, UK	USD 3495 per delegate

► **Available delivery methods:** Face-to-Face & Online Training

Introduction

Ransomware attacks are among the most devastating cybersecurity threats facing organizations today—causing operational shutdowns, data loss, reputational damage, and financial extortion. Proactively auditing ransomware readiness is critical to ensuring cyber resilience and business continuity.

This course equips IT auditors and cybersecurity professionals with the tools to assess and improve an organization’s ransomware defenses. Participants will learn how to evaluate technical controls, test incident response plans, and audit backup and recovery procedures. The training combines frameworks, hands-on simulations, and current threat intelligence to validate preparedness and identify improvement areas.

Objectives

By the end of this course, participants will be able to:

- Understand ransomware attack vectors, stages, and threat actors
- Evaluate the effectiveness of technical and administrative controls
- Audit endpoint protection, segmentation, backups, and recovery strategies
- Review incident response procedures and business continuity plans
- Conduct tabletop exercises and readiness assessments
- Report ransomware preparedness gaps and recommend remediation

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Why Attend

- Strengthen your organization\'s ability to detect, prevent, and recover from ransomware
- Align audit practices with international cybersecurity standards (e.g., NIST, ISO, CIS)
- Learn how to validate controls before a real-world attack occurs
- Analyze case studies of high-profile ransomware incidents
- Provide actionable insights to executive leadership and risk committees

Target Audience

This program is designed for:

- IT Auditors and Cybersecurity Professionals
- IT Risk and Governance Officers
- Incident Response and Business Continuity Managers
- CIOs, CISOs, and Security Architects
- Anyone responsible for cyber assurance and audit readiness

Individual Benefits

Key competencies that will be developed include:

- Ability to perform ransomware-focused IT audits
- Knowledge of ransomware threat landscape and mitigation controls
- Assessment of incident response and recovery readiness
- Execution of ransomware simulation and tabletop audits
- Gap analysis and cyber hygiene auditing

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Improved organizational resilience against ransomware attacks
- Enhanced audit assurance of cybersecurity readiness
- Faster response and recovery from incidents
- Reduced exposure to extortion, data theft, and business disruption
- Better-informed security investments and board-level reporting

Instructional Methodology

The course follows a blended learning approach combining theory with practice:

- Strategy Briefings – Ransomware lifecycle, defense-in-depth, audit roles
- Case Studies – Ransomware breaches and audit failures
- Workshops – Risk assessments, policy reviews, technical audits
- Peer Exchange – Discuss audit scenarios, response gaps, and best practices
- Tools – Audit checklists, simulation templates, NIST CSF-based frameworks

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Course Outline

Training Hours: 7:30 AM – 3:30 PM Daily Format: 3–4 Learning Modules | Coffee breaks: 09:30 & 11:15 | Lunch Buffet: 01:00 – 02:00

Day 1: Understanding Ransomware Risk

- Module 1: Anatomy of a Ransomware Attack (07:30 – 09:30) • Infection vectors, lateral movement, encryption stages
- Module 2: Threat Landscape and Common Attack Methods (09:45 – 11:15) • Phishing, RDP attacks, supply chain infiltration
- Module 3: Regulatory Implications and Audit Responsibilities (11:30 – 01:00) • GDPR, NIS2, SEC, and financial sector mandates
- Module 4: Workshop – Map the Ransomware Kill Chain (02:00 – 03:30) • Participants build attack lifecycle scenarios

Day 2: Controls and Prevention Audit

- Module 5: Endpoint and Perimeter Protection Review (07:30 – 09:30) • Antivirus, EDR, firewalls, DNS filtering
- Module 6: Access Control, Privileged Account Audit (09:45 – 11:15) • Zero trust, MFA, PAM systems
- Module 7: Network Segmentation and Threat Detection (11:30 – 01:00) • Segregation testing, SIEM, anomaly detection
- Module 8: Workshop – Perform a Control Audit Using a Checklist (02:00 – 03:30) • Evaluate a simulated environment

Day 3: Incident Response and Recovery Readiness

- Module 9: Incident Response Plan Audit (07:30 – 09:30) • Chain of command, containment, investigation
- Module 10: Backup Systems and Recovery Controls (09:45 – 11:15) • Air-gapped backups, immutability, recovery testing
- Module 11: Communication and Escalation Protocols (11:30 – 01:00) • Notification, legal considerations, media
- Module 12: Workshop – Simulate an IR Audit (02:00 – 03:30) • Gap identification from a ransomware event log

Day 4: Simulation and Risk Assessment

- Module 13: Conducting a Ransomware Tabletop Exercise (07:30 – 09:30) • Facilitation, role play, injects
- Module 14: Cyber Insurance and Legal Audit Considerations (09:45 – 11:15) • Coverage gaps, claims audits, forensic readiness
- Module 15: Ransomware Risk Assessment Methodology (11:30 – 01:00) • Scoring impact, likelihood, and control maturity
- Module 16: Workshop – Conduct a Tabletop Review (02:00 – 03:30) • Participants facilitate and debrief a ransomware scenario

Day 5: Reporting and Improvement Planning

- Module 17: Reporting to Executives and Boards (07:30 – 09:30) • Heat maps, dashboards, metrics
- Module 18: Gap Closure and Continuous Monitoring (09:45 – 11:15) • Remediation planning, audit trail maintenance
- Module 19: Case Study – Ransomware Failure and Response Analysis (11:30 – 01:00) • Post-mortem evaluation of high-profile attack
- Module 20: Final Workshop – Prepare a Ransomware Readiness Audit Report (02:00 – 03:30) • Teams present audit findings and recommendations

Certification

Participants will receive a Certificate of Completion in Ransomware Preparedness Audit, validating their ability to evaluate, audit, and strengthen an organization\'s ransomware defense posture across technical, procedural, and governance layers.

Why Choose MAWA Events

- **Global Expertise:** More than 17 years of experience in professional training and consulting.
- **Industry-Leading Faculty:** Courses delivered by seasoned professionals with hands-on experience.
- **Practical Insights:** Learn to turn theory into actionable strategies for real-world business impact.
- **Client-Focused Solutions:** Customized programs designed to achieve your organisation’s unique goals.

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

In-House / Customized Training Interested in running this course for your team? Please contact us:	TEL: **+601116373203**	EMAIL: **info@mawaevents.net**