CONCEPT

Cyber Law and IT Law: Cybercrime Offences, Electronic Evidence and Platform Liability

1 – 5 November 2027
London - Central London four-star



Cyber Law and IT Law: Cybercrime Offences, Electronic Evidence and Platform Liability

Ref: 743_19417 **Date:** 1 – 5 November 2027 **Location:** London - Central London four-star **Fees:** 23000 SAR

Introduction:

A ransomware intrusion, a leaked customer file or a fake executive account raises legal questions faster than most organisations can answer them: which cyber law offence has occurred, whether the company itself is exposed, what electronic evidence must be kept intact, who must be notified and which jurisdiction applies. This Core Concept course gives in-house counsel, compliance and IT governance staff a working grasp of cyber law and IT law, from cybercrime offence categories to platform liability and cross-border cooperation. Participants draft a Cyber Incident Legal Response Memo for a case breach.

Course Objectives:

- Classify an incident against the cybercrime offence categories of illegal access, interception, data and system interference, misuse of devices, computer-related forgery and fraud
- Assess corporate criminal and civil exposure arising from staff, contractor and third-party conduct online
- Advise on the admissibility, integrity and chain of custody of electronic records relied on in disputes and prosecutions
- Apply intermediary safe-harbour conditions and a notice-and-takedown procedure to hosted content, domain names and software products
- Determine incident notification duties, cross-border jurisdiction and cooperation routes under the Budapest Convention on Cybercrime
- Draft a Cyber Incident Legal Response Memo setting out offences, exposure, evidence steps, notifications and recommended actions

Target Audience:

- In-house legal functions that advise management on cyber incidents, online misconduct and technology disputes
- Compliance functions responsible for breach reporting, regulatory correspondence and policy enforcement
- IT governance and information security policy functions that write acceptable use, monitoring and incident rules
- Risk and internal audit functions that assess legal exposure from technology operations and suppliers
- Digital platform and product managers who host user content, run domains or ship licensed software

Course Outline:

Day 1: Scope of Cyber Law and IT Law and the Cybercrime Landscape

- IT Law Scope Map: Cybercrime, Electronic Evidence, Intermediaries, Domains and Software
- Computer Data, Computer System and Traffic Data Definitions in Cybercrime Instruments
- Criminal Versus Civil Routes for Online Wrongs: Remedy Selection Matrix
- Cyber Incident Legal Exposure Register for a Mixed-Sector Organisation
- Current-State Review of Acceptable Use, Monitoring and Incident Reporting Policies

Day 2: Cybercrime Offence Categories and Corporate Liability

- Budapest Convention Offence Structure: Illegal Access, Illegal Interception and Data Interference
- System Interference and Misuse of Devices: Intent, Authorisation and Exceptions
- Computer-Related Forgery, Computer Fraud and Identity Misuse Elements Test
- Online Defamation and Harassment Offences: Publication, Identification and Defences
- Corporate Liability Model: Attribution of Employee Acts, Supervision Failures and Sanctions

Day 3: Electronic Evidence, Records Protection and Chain of Custody

- Admissibility Tests for Electronic Records: Authenticity, Integrity and Best Evidence
- Chain of Custody Log: Collection, Hash Verification, Storage and Transfer Records
- Litigation Hold Notice and Preservation Request for Logs, Mailboxes and Cloud Data
- Protection of Electronic Documents: Unauthorised Alteration, Destruction and Disclosure Remedies
- Expedited Preservation and Production Order Procedures in the Budapest Convention

Day 4: Intermediary Liability, Domain Names, Software and Notification Duties

- Intermediary Safe-Harbour Conditions for Mere Conduit, Caching and Hosting Services
- Notice-and-Takedown Workflow: Notice Validity, Counter-Notice and Repeat-Infringer Records
- Domain Name Disputes: Cybersquatting, Bad-Faith Registration and Administrative Complaint Route
- Software Licensing Liability: Warranty Disclaimers, Defect Claims and Licence Breach Remedies
- Incident Notification Duty Matrix: Regulators, Data Subjects, Counterparties and Insurers

Day 5: Cross-Border Cases and the Cyber Incident Legal Response Memo

- Jurisdiction Analysis Grid: Location of Server, Victim, Offender and Data
- Mutual Legal Assistance and the Budapest Convention 24/7 Network Referral Route
- Case Breach File Review: Business Email Compromise at a Logistics Operator
- Cyber Incident Legal Response Memo Drafting: Offences, Exposure, Evidence and Notifications
- Legal Review Panel: Memo Defence, Challenge Questions and Action Priorities

Skills You Will Gain:

- Cybercrime Offence Classification
- Corporate Cyber Liability Assessment
- Electronic Evidence Admissibility Review
- Chain of Custody Documentation
- Intermediary Safe-Harbour Analysis
- Domain Name Dispute Handling
- Breach Notification Planning
- Cross-Border Jurisdiction Mapping

Why Attend This Course:

- Leave with a Cyber Incident Legal Response Memo template tested on a realistic breach file
- Give management a clear legal position within hours of an incident instead of waiting for outside counsel
- Keep electronic records usable in court by setting legal preservation steps before systems are rebuilt
- Compare cyber law practice with legal, compliance and governance peers from banking, logistics, retail, telecoms and public services

Conclusion:

Cyber incidents turn into legal problems the moment data is taken, altered or published. The week moves from the scope of IT law and the cybercrime offence categories, through corporate liability and the legal rules on electronic evidence and chain of custody, to intermediary safe harbours, notice-and-takedown, domain name disputes, software liability and notification duties, and then to cross-border jurisdiction and cooperation under the Budapest Convention. The final day produces a Cyber Incident Legal Response Memo ready for use. The course covers general principles and is not legal advice.