PR, MEDIA AND MARKETING

PR16 Cybersecurity for Non-IT Leaders

In today's digital age, organisations face ever-evolving cyber threats that necessitate a proactive and vigilant approach to cybersecurity. This comprehensive course is meticulously crafted to equip delegates with the essential knowledge and practical skills required to mitigate cyber risks effectively. By fostering a culture of cybersecurity awareness and understanding, participants will learn to identify, assess, and address cyber threats within their organisations. Through a blend of theoretical insights and hands-on exercises, this course aims to empower delegates with the tools and strategies necessary to enhance organisational resilience and protect critical assets from cyber-attacks.

Course Information

Duration: 5 days

London (£4950): 22nd June 2026, 5th October 2026, 1st February 2027

Companies nominating 3 or more delegates to attend the same programme will enjoy a special discount on the course fees.

Upon completion of one of our CPD certified courses, delegates will be awarded both an LMC certificate and a CPD certificate. No examination required.

Who is the course suitable for?

This course is tailored for senior staff seeking a comprehensive overview of cybersecurity best practices, as well as Communications Professionals engaged in marketing, PR, and the Media. It is also ideal for subject matter experts, technical specialists, or leaders of teams specialising in critical areas, ensuring they stay at the forefront of their respective fields.

Course profile

Understanding Cyber Risk

- Introducing cyber risk fundamentals
- Assessing different types of cyber risk
- Appreciating the consequences of cyber attacks
- Making cybersecurity everyone's responsibility
- Disseminating and communicating cyber risk awareness across the organisation

Dealing with Cybersecurity Threats

- Creating organisational cybersecurity policies and procedures
- Identifying malicious activity and cyber threats
- Mitigating cyber threats effectively
- Assessing and validating essential cybersecurity documents
- Monitoring and administering cyber security threats

Organisational Risk Culture

- Defining the importance of risk culture in cybersecurity
- Implementing cybersecurity governance frameworks
- Establishing cyber risk appetite and tolerance levels
- Clarifying roles and responsibilities for cybersecurity within the organisation

Third Party Threats

- Evaluating cyber risks associated with third-party organisations
- Designing and implementing measures to mitigate third-party risks
- Auditing third-party arrangements for cybersecurity compliance
- Reviewing and advising on security measures for third-party engagements

Incident Management and Business Continuity Planning

- Understanding the incident management process
- Developing effective business continuity plans
- Conducting business impact analysis
- Testing and maintaining continuity plans for organisational resilience

Competencies

At the end of this course, delegates will be able to:

- Assess various types of cyber risks within their organisation.
- Implement effective cybersecurity policies and procedures to protect assets.

- Spot and mitigate malicious activities and cyber threats.
- Cultivate a robust organisational risk culture conducive to cybersecurity.
- Evaluate cyber risks associated with third-party organisations and implement appropriate measures to mitigate them.
- Manage incidents effectively through comprehensive incident management processes.
- Develop, test, and maintain business continuity plans to ensure organisational resilience.
- Disseminate cybersecurity awareness and communicate effectively across the organisation.

Course Booking

Call us: +44 (0) 207 724 6007

Email us: training@lmcuk.com

www.lmcuk.com

RESERVE A PLACE