



I. COURSE

This seminar is dedicated to:

- The context of Cyber Security with a focus on your industry
- The definition of holistic Cyber Security and the key role of Leadership
- Leadership theory and practice in relation to Cyber Security
- The current and evolving Cyber Security landscape and relevant Threats
- Working with a 'cross leadership' understanding and model to develop effective risk mitigation strategies
- Overview of pertinent legislation, risks and liabilities
- Leadership, Strategy and best practice Information Governance
- Responsibilities and key stakeholder relationships including a clear and comprehensive understanding of the role of Senior Leaders
- Business Information Risk Management
- Business Resilience and Incident Management
- Leading change in Cyber Security context
- Cyber Security and the human behaviour model
- Best practice to foster a positive Cyber and Information Security culture encompassing people, policy, process as well as Information and Communications Technology (ICT)
- Leading effective communications strategy to support holistic Cyber Security approaches
- Management Information systems and their role in defining leadership practice and response

2. COURSE CONTENT

All levels of leadership within the organisation need to create policy, strategy and plans that enable effective exercise of accountability, ownership, management, assurance and reporting.

There are numerous factors affecting human interaction with better Cyber Security practices.

Often these behaviours are seen as 'blockers' to engagement and therefore progress.

Understanding leadership and its interactions with the workforce is crucial to embedding good Cyber Security practices across a business or organisation.

Delegates will develop a deep understanding of leadership responsibilities and practices to mitigate Cyber risks and ensure business continuity and organisational resilience.

3. COURSE FORMAT

Learners will engage in an interactive workshop which will allow them to develop theoretical knowledge and apply it to their own situations. Delivery will be through a blended approach that will allow learners to fully engage in the session and gain practical examples of how to turn theory into practice.

4. DETAILED COURSE PROGRAM

Delivery will progress the theoretical and knowledge base of the required modules for the formal qualification. Sessions will be spread across the five days and progress at the pace of the learners using detailed activities that both develop practical application and real life implementation of the learning.

5. COURSE PREPARATION

Learners should be familiar with their organisation's Information Governance structures, Policies and Procedures and demonstrate engagement in leadership theory and practice around Cyber Security risk and threats.

6. COURSE EVALUATION

Participant engagement and contribution is essential in this course. It is expected that all learners fully interact with the learning and the group activities.



7. BIOGRAPHY

All course tutors will have the following professional credentials.

- UK National Cyber Security Centre Certified Trainers
- Higher level professional and teaching qualifications, gained over a career in Cyber Security practice.
- Contribution to the profession, giving back to the community at large, through voluntary engagement and seats on esteemed industry panels, working groups and special interest groups.
- Wide experience of professional roles in Cyber Security, leading to national and in many cases international reputations in domain.
- A complete and extended understanding of Cyber Security, Information Governance across a number of sectors
- A wide-ranging understanding of Finance and Procurement in relation to Cyber Security related practices

Our experienced, expert and engaging NCSC and Executive Trainer pool includes the following profiles:

NCSC Certified and Executive Trainer: Experienced strategy adviser and solution implementer, with international leadership experience in both government and commercial organisations. Over 22 years' experience in the fields of Cyber Security, Information Assurance and Information and Communications Technology after a background in Computer Science and Computing Information Systems. A Visiting Teacher of Cyber Security at the Oxford Martin School of Oxford University. Leads on audits and compliance-related activities with a focus on Critical National Infrastructure, including Central Government and Law Enforcement.

NCSC Certified Executive Trainer: Extensive financial services sector, developing Cyber Security and Information Assurance strategies, delivering Board briefings, leading audits and training and mentoring Senior Executives. Clients include G7 banks, central banks, retail banks and private equity firms. A thought leader in the area of Cyber Security and Information Assurance, speaking at conferences with articles regularly published. A visiting Professor at Oxford University.



NCSC Certified and Executive Trainer: Extensive experience includes mentoring Senior Executives in both the private and public sector. An established and highly effective leader with operational and commercial experience spanning private and defence sectors in the UK, Europe and the Middle East. Led Cyber Health Checks and Audits for multi-national clients, identifying key Cyber risks and threats and advising on improving Cyber resilience.

NCSC Certified and Executive Trainer: Expertise and experience in delivering training and workshops to Board and senior audiences across government and the commercial sector. Background includes geopolitical risk and global threats, information risk and security, as well as risk mitigation, crisis management and prevention. Fostered networks for sharing best practice with Cyber Security organisations in the US, the EU and across the Commonwealth and was a member of the Cyber Assessment Advisory Panel at the UK National Cyber Security Centre (NCSC).

NCSC Certified and Executive Trainer: coaches and trains leadership on Cyber and Risk across sectors and in the Critical National Infrastructure. Brings significant operational and field experience to his practitioner and academic work and specialises in the human dimension of cyber security. Previously, he was Chief Executive of a UK national body and author of a number of Cyber Security books sold internationally.

NCSC Certified and Executive Trainer: Experience of wide ranging organisational support. Advises on information governance policy development and Cyber Security leadership and strategy. Background in education, academia and the not-for-profit sector has seen him advise government on national skills strategies and develop skills programmes in Cyber Security across the UK. Vice Chairman of the Information Assurance and Advisory Council. Working with national and regional bodies, and private sector parties, he focuses on developing regional cyber resilience strategy. Recipient of a National Cyber Security Award for his work with young people and cyber security.