



1. COURSE

Ce séminaire est consacré à :

- The latest Threat briefing and trends; including Social Engineering
- The key role of Senior Executives to deliver Cyber Security maturity and resilience; and managing internal and external stakeholder relationships
- Leadership, Strategy and Governance
- An understanding of responsibilities, liabilities, and consequences of breach, including key legislation
- The importance of Business Information Risk Management
- Building Cyber resilience and capability; including Incident Management
- Scenarios to support understanding and consolidate learning
- A trusted forum to discuss key issues and priorities.

2. COURSE CONTENT

Senior Executives play a critical role in any organisation, and as the threat landscape evolves, Senior Executives need to develop a greater awareness of Cyber risks and threats. Leadership is pivotal to drive and champion holistic Cyber Security and Information Assurance to ensure that an organisation develops its Cyber Security maturity; enhances and embeds a positive information culture across the organisation; and demonstrates continuous improvement in a dynamic environment.

Senior Information Risk Owners (SIROs) are often designated as the Board-level representative to take the lead on managing Cyber risks. With two thirds of businesses suffering cyber attacks in the last year, and the heightened cyber threat due to the current geo-political situation, it is imperative that senior leaders own the responsibility for Cyber risk and promulgate the right attitude across their organisation. Developing Senior Executive level ownership for information risk will quickly establish business resilience and help mitigate risks that could be detrimental to any organisation.

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 (unrolled training sequences)

| Session | Delivery |
|---------|--|
| 1 | Inroduction |
| 2 | The Leadership Challenge Overview of the roles and responsibilities involved in information governance and data assets |
| 3 | Current Legislation An overview of current legislation and the associated liabilities, regulations, standards and the consequences of non-compliance |
| 4 | Cyber Threats and Risks An in depth look at the current Cyber threats and risks surrounding information governance and data assets – focusing on key senior individuals as well as organisation-wide |
| 5 | Vulnerability Analysis Deciding where the vulnerabilities exist in an organisation and looking at how organisations can develop a prioritised roadmap these for mitigating actions |
| 6 | Developing a Holistic Cyber Security Approach Establishing best practice and developing ways if implementing an organisation wide strategy to both own and reduce Cyber riskn |
| 7 | Course Summary and Evaluation |

5. COURSE PREPARATION

Candidates will be in new and existing Senior Executive roles or appointed as Senior Information Risk owners. The course will also be applicable for those appointed to a leadership or governance role in respect of Cyber and Information Risk.



6. EVALUATION DU COURS

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 Cyber Security laws the related legislation surrounding
- international expectations

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.