One Day – Cyber Security & Crisis Management

Maritemex
Holistic Cyber Security Resilience

1. COURSE

This seminar is dedicated to:

- The importance of Cyber Security in an organisational context;
- The dynamic Cyber threat landscape. Includes latest threats, such as cyber fraud, malware, ransomware, social engineering, insider threat and COVID-19 themed phishing attacks; and future trends;
- Overview of key legislation and obligations; and the impact of non-compliance - financially, operationally and reputationally;
- Types of Cyber Security incidents and the importance of a holistic approach, encompassing people and culture, policy, processes and ICT;
- Incident Management processes and Incident Management roles and responsibilities;
- Key actions and lines to take in response to Cyber Security incident/s to manage and control the potential crisis;
- Discussion and understanding of key stakeholders, engagement and timing;
- Real-life scenarios from Templar's extensive experience and other case studies to consolidate learning; with practical tips and exercises;
- Discussion and Q&A to support personal and team action.
-

2. COURSE CONTENT

Cyber attacks are now classed as the top threat to organisations. With the average cost of a cyber attack being close to 2 million MAD the financial implications for businesses cannot be ignored. It's not just the financial loss that could adversely impact organisations but also the damage to brand, reputation and continued business operations. t Without proper planning, a Cyber-attack could therefore be devastating.
This dynamic Crisis Training course incorporates the planning and testing of Crisis Management Plans to ensure preparedness, understanding of roles and responsibilities, communication and stakeholder engagement, and continuous improvement.
This training prepares participants to respond to issues related to a Cyber Incident. This training course covers emergency tools and procedures to better respond to cyber attacks on a legal and organizational level.

The participants of the Crisis Management training will be able to address the fundamentals and specificities of cyber crisis management. All the information dealt with will be applied in the context of a practical case.

3. COURSE FORMAT

Learners will engage in an interactive workshop supported by crisis exercise scenario and role-playing.

4. DETAILED COURSE PROGRAM (unrolled training sequences)

Session	Delivery
1	***Introduction to cyber security and crises***
2	***Risk – reputational, regulatory & compliance, financial impact***
3	***Crisis context (supported by exercise)***
4	***Crisis context (supported by exercise)***
5	***Best practice***
6	***Next steps discussion to embed crisis planning into Cyber Security***
7	***Course Summary and Evaluation***

5. COURSE PREPARATION

This course is open to anyone responsible for leading, managing or assisting in the response to Cyber Security related crises and incidents.

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: c**oaches 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 oganisational 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.