Cyber Attacks – the Risk and the Fix

Over two days, delegates are shown the reality of just how easy real cyberattacks can be – even those with the most devastating effects – and the implementation of simple measures to avoid catastrophic risk. The practical elements are comprehensively taught in a walk-through manner to demonstrate the vulnerabilities in realistic targets. A key theme running through the course is that of workforce vulnerability – no matter how well defended the organisation's intellectual property is, the staff are the way in.

Designed for:
Government, business, critical infrastructure, banking, transportation, energy, shipping and ports, retail, leisure, police, intelligence and security operations whether government or private sector. The case studies and work will be drawn from Europe, Africa, Middle East and South Asia depending on the persons attending and the region where the course is delivered.

The course is suitable for entirely non-technical officers as well as cyber managers and administrators who wish to develop a sound understanding of just how easy and low-tech the efforts of an attacker can be, and how to implement mitigation or who wish to upgrade their existing skills to become more cost effective for their organisation.

Day One – The Risk

- **Introduction to Cyber Risk**
- **Attacker Methodology**
  Part One – reconnaissance
  Part Two – Attack
- **The Persistent Threat of Leaked Data**
- **Wi-Fi – the Corporate and Personal Risk**

Day Two – The Fix

- **Real world examples of damaging attacks are dissected, with particular emphasis on correct implementation of cyber incident response**
- **Exercise: Attack the Corporation. The art of incident response**
- **The Devastation.** Lessons learned from a vast number of cyber incident responses
- **The technical penetration test – learning why most companies waste time and money with incomplete or ineffective testing**

About the trainer: **North Cyber** are team of former intelligence officers with expertise in covert online operations and digital forensics. The company teaches government and corporate clients how find and fix the unseen holes in their security. They specialise in all levels of capability including low-tech and no-tech hacking, using freely available information to circumvent vastly expensive but ineffective security systems. The teaching draws on many and varied real-world examples from the private and government sectors, from the perspectives of the attacker and incident responder. Participants in these courses will evaluate their own experience on the course in gaining additional skills and understanding of the threats to their organisation and they will gain confidence in tackling these catastrophic risks to the comparate or government operation.

Details

Duration:	**2-day training course 2018**
London:	**2-3 July; 1-2 October**
Amsterdam:	**9-10 July; 8-9 October**
Abu Dhabi:	**16-17 July; 22-23 October**
Johannesburg:	**23-24 July; 29-30 October**
Singapore:	**10-11 September**
Sectors:	**All – especially for Governments and Critical National Infrastructure Companies**

Available as bespoke in-house training

For pricing and further information:
+44 (0)20 7936 8989 teampulse@pulseconferences.com www.pulseconferences.com

The Threat from Business Espionage

Module 1 – discusses what intelligence is, who collects it and methods of intelligence gathering.

- Overview of intelligence
- Who collects intelligence and why
- Methods of intelligence collection

Designed for:
Designed to develop new skills and knowledge for corporate operations and security managers at all levels of management.

Module 2 – discusses physical and information security methods, the insider threat and counter intelligence and how security is compromised by human nature.

- Physical and Information security methods
- Counter intelligence and the insider threat
- How security is compromised by human nature

Module 3 – is a series of case studies through the medium of role playing exercises and case studies.

- Role playing of intelligence gathering techniques and security responses
- Theory and practical exercises
- Case studies

About the trainer:
Robert Shaw is a security, intelligence and EOD executive with a UK Military background. He has broad strategic and operational experience and has advised senior staff, diplomats and government officials on aspects of security, intelligence, threat analysis, crises management, and resilience strategies. He has been the UN Security and EOD Advisor; Liaison officer for the UNMAS and UNOPS and has experience with NATO, the GCC, African Union, OSCE, EUPOL, FCO and others. Robert is a respected expert, has specialist research background on suicide bombing and has provided thematic briefs on worldwide security issues relevant to UNMAS/UNOPS missions.

Details

Duration:	**2-day training course 2018**
London:	**4-5 July; 3-4 October**
Amsterdam:	**11-12 July; 10-11 October**
Abu Dhabi:	**18-19 July; 17-18 October**
Johannesburg:	**25-26 July; 31 October-1 November**
Singapore:	**12-13 September**
Sectors:	**All**

Available as bespoke in-house training

For pricing and further information:
+44 (0)20 7936 8989 teampulse@pulseconferences.com www.pulseconferences.com

Security & Resilience Leadership and Management Training

Module 1 – discusses the perceptions of leadership, management and command. Different levels of management and styles. What people expect from their leaders and differing organisational structures and functions.

- Overview of leadership management and command and their links to culture
- Levels of command and styles of management
- Organisational structures and functions
- Personnel and organisation expectations

Designed for:

This training is designed to develop new skills and knowledge for corporate and government personnel that lead and manage teams at all levels.

Module 2 – discusses personality types, recruitment strategies and interviewing techniques, managing expectations and attitudes, methods of communication, the threat from disgruntled personnel, the techniques of coaching and mentoring and how to manage change.

- Personality types and team building.
- Recruitment strategies and interviewing techniques.
- Managing expectations and attitudes.
- Methods of communication.
- The threat from disgruntled personnel.
- Coaching and mentoring.
- Managing change.

Module 3 – is a series of case studies through the medium of battlefield tours, role plays and management exercises.

- Role playing of management techniques and responses.
- Theory and practical management exercises.
- Case studies

About the trainer: Robert Shaw is a security, intelligence and EOD executive with a UK Military background. He has broad strategic and operational experience and has advised senior staff, diplomats and government officials on aspects of security, intelligence, threat analysis, crises management, and resilience strategies. He has been the UN Security and EOD Advisor; Liaison officer for the UNMAS and UNOPS and has experience with NATO, the GCC, African Union, OSCE, EUPOL, FCO and others. Robert is a respected expert, has specialist research background on suicide bombing and has provided thematic briefs on worldwide security issues relevant to UNMAS/UNOPS missions.

Details

Duration:	**2-day training course 2018**
London:	**6-7 August**
Amsterdam:	**8-9 August**
Abu Dhabi:	**18-19 November**
Johannesburg:	**26-27 November**
Singapore:	**29-30 November**
Sectors:	**All**

Available as bespoke in-house training

For pricing and further information:

+44 (0)20 7936 8989 teampulse@pulseconferences.com www.pulseconferences.com

Resilience Communications Training – Media, Brand Protection, Crisis Governance

Module 1 – New Threats – covers on new threats to energy and critical infrastructure, railways, aviation, shipping and ports, construction of buildings and to the financial and government centres of major cities. Catastrophic hazards that often generate media inquiries include internal issues within the corporation or government department, large transformation projects, major infrastructure construction, terrorism, cyber- attacks, extreme weather events, insider threats, security, organised crime and fraud and events such as Brexit, North Korea's nuclear weapons programme, mass population movements, and military exercises close to national borders.

Module 2 – Optimising Communication Strengths is a practice session for all the participants to identify their strengths in contributing to a media and brand resilience process. This could be gathering information and team leadership or presenting information to internal staff, stakeholders or preparation of information for spokespersons to use in media statements.

Designed for: *Resilience communications are taught in a fast-track one-day session to develop new skills and knowledge for corporate and government personnel.*

Module 3- Governance for Crisis Communications brings together all the phases of a catastrophic event with new governance principles that will assist in reporting after an incident on how processes were successfully managed to contribute towards the brand protection and resilience operations of the organisation.

- Governance Principles relevant to the Communications Plan
- Analysing Feedback
- Regular timing of messages and trust building
- Recognising hostility and reducing tensions
- Assessing effects on the Brand and reducing losses

About the Instructor:

Dr. Sally Leivesley is an expert in catastrophic risk and security for protection of life and critical infrastructure. She provides around 100 interviews to media a year on extreme events and communicates on public safety issues. She has been providing commentary to the BBC World Service and many other media outlets since 9/11 and commenced her media communications work when tasked with recovering a city after a severe weather disaster. Her media work includes real time commentary during extreme life threatening events such as the Beslan school terror attack and in the immediate aftermath of terrorist and other incidents such as the flight MH17 aviation incident, Mr. Litvinenko's radiation poisoning, natural disasters, threats such as DPRK nuclear programme, terror attacks in France and Brussels, Britain's 7/7 and 21/7underground rail terror attacks and she covers most major incidents of importance to the public in any year. She has worked in catastrophic risk assessments and training within critical infrastructure covering many industries including energy, petrochemicals, rail, aviation, shipping, banking, government emergency planning and nuclear, chemical, biological and radiological incidents. (www.Newrisk.com Recent Media Commentary).

Details

Duration:	**2-day training course 2018**
London:	**13-14 August; 29-30 November**
Amsterdam:	**8-9 October**
Abu Dhabi:	**18-19 November**
Johannesburg:	**26-27 November**
Singapore:	**29-30 November**
Sectors:	**All**

Available as bespoke in-house training

For pricing and further information:

+44 (0)20 7936 8989 teampulse@pulseconferences.com www.pulseconferences.com

New Principles for Governance and Strategy in a Crisis

New governance principles help senior managers understand strategy and make decisions in a crisis. The five new Governance steps taught in this course build a general crisis governance framework for government and business.

You will learn the operational decision making skills for each Governance Principle. Alongside the theory, the know-how is taught through scenario exercises so each participant will become confident over the two days in how to apply the new governance principles for the benefit of their workplace. It is well recognised that when insider threat actors, criminals, terrorists, nation states or natural disasters impact on a country it is the experience and know-how of team leaders that prevent losses and strengthen government and business response. Strategic decision making is rarely offered in training but participants will personally develop new skills when studying each of the five new governance principles and benefiting from peer-to-peer discussions and solutions based on their experience.

Module 1: Governance when building a Risk Framework
Module 2: Trust and Assurance
Module 3: Interface with Board and Stakeholders
Module 4: Crisis Management and Recovery

Designed for: *CISOs, CSOs, COOs, senior managers in finance, planning, government policy planners and senior officers in intelligence, emergency services, defence and cyber security, innovators in disruptive technologies, AI, IOT, banking, internal auditors, insurance and financial services, post-graduate students in Masters and higher degree courses, cyber security technology vendors and designers. The course is strongly based on peer-to-peer learning and practical tests to build capability and confidence in their leadership skills and strategic decision making that will benefit the employer and the stakeholders in their organisation.*

About the instructors:

Nigel Somerville MBE MC, Linton Dragon Limited and TEG7 LLP
Nigel has a UK Military background with significant cross-cutting security experience in the most challenging of land and maritime environments. He holds strategic experience providing ministerial advice to Whitehall, COBR and the Cabinet Office on security risk. Masters educated and appointed to the Register of Chartered Security Professionals (CSyP) his focus is counter-terrorism, crowded space threat management, security by design and the cyber-physical threat within the built environment. He studies the tactics and vulnerabilities that terrorists have exploited in recent complex attacks to inform crisis planning and prevent catastrophic impact.

Dr Sally Leivesley PhD Lond., MSPD, BA(Hons) Qld., FICPEM, FRSA, MACE, MIABTI, Director, Newrisk Limited and TEG7 LLP
Sally has a UK Home Office background and trained as a Scientific Advisor to respond to all aspects of nuclear attack and chemical, biological and radiological events. She plans, directs and participates in major exercises concerning critical components of industry and specialises in testing catastrophic threat impacts on critical functions of business. She has experience in all phases of risk assessment, planning, crisis management and post-loss recovery including psychological interventions in communities, post-disaster. Sally is a respected media adviser on public protection and is a member of the Register for Security Engineers and Specialists (RSES).

Details

Duration:	**2-day training course 2018**
London:	**15-16 August; 3-4 December**
Amsterdam:	**8-9 October**
Abu Dhabi:	**18-19 November**
Johannesburg:	**26-27 November**
Sectors:	**All**

Available as bespoke in-house training

For pricing and further information:

+44 (0)20 7936 8989 teampulse@pulseconferences.com www.pulseconferences.com

Cyber Security for Ports and Vessels

With the increasing use of information and communications technology (ICT) in the port and maritime sectors, and the connection of operational technologies (OT) such as control systems, there is a need to address the cyber security issues. The IMO's ISPS Code requires port and vessel operators to put in place appropriate controls and supporting business practices to address security risks, including those that are cyber related. This course is based on the UK Department for Transport (DfT) sponsored Codes of Practice for Cyber Security of Ports and Port Systems, and Vessels, that were prepared by the Institution of Engineering and Technology (IET).

The objectives of the course are to enable delegates to:

- understand and appraise the cyber security threats to their port or maritime operations;
- undertake a risks assessment of their cyber-physical systems and operations;
- develop an appropriate and proportionate security strategy, management plan.

Module 1: The cyber security threat
Module 2: Cyber security for ports
Module 3: Cyber security for vessels
Module 4: Developing and maintaining cyber security assessment and plan

About the instructor:
Hugh Boyes BSc(Hons) MBA CEng FIET CISSP
Hugh is a Chartered Engineer, a Fellow of the Institution of Engineering and Technology (IET) and holds the Certified Information Systems Security Professional (CISSP) credential issued by the International Information Systems Security Certification Consortium [(ISC)2]. He divides his time between working as a Principal Engineer at the University of Warwick and undertaking cyber security training and consultancy assignments. Hugh is an industry expert on cyber threats to cyber-physical systems, including those in the built environment, ports and maritime sectors. He has written four guidance documents for the IET covering cyber security in the built environment, ports and vessels. His research work focuses on the protection of control systems, whether traditional industrial controls or employing IoT technologies. He is the co-author of British Standard's PAS 1192-5:2015 [Specification for security-minded building information modelling, digital built environments and smart asset management] and PAS 185 [Smart Cities – Specification for establishing and implementing a security-minded approach]. He regularly reviews standards to assess their handling of security issues and sits on the drafting committee for the forthcoming British Standards BS10754 suite of documents. Hugh is a Member of the Register of Security Engineers and Specialists (RSES).

Details

Duration:	**2-day training course 2018**
London:	**15-16 August; 3-4 December**
Amsterdam:	**8-9 October**
Abu Dhabi:	**18-19 November**
Johannesburg:	**26-27 November**
Sectors:	**All**

Available as bespoke in-house training

For pricing and further information:
+44 (0)20 7936 8989 teampulse@pulseconferences.com www.pulseconferences.com

Cyber Policy and Standards for Systems Security

In a rapidly changing business and technical environment the choice of standards and codes of practice can make a significant difference to the success of your organisation. There are a range of existing cyber security related standards, publicly accessible specifications (PAS) and codes of practice. The choice of whether to implement specific standards can have a significant impact on your organisation's costs and performance.

The objectives of the course are to enable delegates to:

- examine the nature and role of standards, publicly accessible specifications and codes of practice;
- review of the security standards landscape;
- understand factors to be taken into account when implementing standards, both within the organisation and supply chain.

Module 1: The nature and roles of standards
Module 2: Understanding testing, validation and verification
Module 3: The security standards landscape
Module 4: Choosing and using standards

About the instructor:
Hugh Boyes BSc(Hons) MBA CEng FIET CISSP is a Chartered Engineer, a Fellow of the Institution of Engineering and Technology (IET) and holds the Certified Information Systems Security Professional (CISSP) credential issued by the International Information Systems Security Certification Consortium [(ISC)2]. He divides his time between working as a Principal Engineer at the University of Warwick and undertaking cyber security training and consultancy assignments. Hugh is an industry expert on cyber threats to cyber-physical systems, including those in the built environment, ports and maritime sectors. He has written four guidance documents for the IET covering cyber security in the built environment, ports and vessels. His research work focuses on the protection of control systems, whether traditional industrial controls or employing IoT technologies. He is the co-author of British Standard's PAS 1192-5:2015 [Specification for security-minded building information modelling, digital built environments and smart asset management] and PAS 185 [Smart Cities – Specification for establishing and implementing a security-minded approach]. He regularly reviews standards to assess their handling of security issues and sits on the drafting committee for the forthcoming British Standards BS10754 suite of documents. Hugh is a Member of the Register of Security Engineers and Specialists (RSES).

Details

Duration:	**2-day training course 2018**
London:	**15-16 August; 3-4 December**
Amsterdam:	**8-9 October**
Abu Dhabi:	**18-19 November**
Johannesburg:	**26-27 November**
Sectors:	**All**

Available as bespoke in-house training

For pricing and further information:
+44 (0)20 7936 8989 teampulse@pulseconferences.com www.pulseconferences.com

Catastrophic Risk Theory and Practice for Energy, Leisure and Transportation

Catastrophic risk methodology delivers high value through integrated risk assessments which reduces costs. The course applies an 'all-risks' approach that adds value to commercial and government operations. Through an all-risks approach, business operations can be sustained in many new ways. This novel approach will give course participants an opportunity to be innovative with solutions to prevent and respond to extreme threats.

Designed for; Energy, leisure and transportation sectors are critical to the productivity of nations in the region. A course on catastrophic risk theory and practical work with case studies is offered to CISOs, CEOs, CSOs, COOs, finance managers, Board Directors, auditors, City Planners and policy experts, intelligence experts, big data analysts, financial technology developers, mobile data and financial services, team leaders and senior managers and first responders to incidents.

The two-day catastrophic risk course covers methodology to quantify risks that threaten critical operations of energy, leisure and transportation infrastructure. The course takes participants beyond general risk frameworks they are already using to understand the value of adding procedures to sustain their operations when catastrophic events threaten the survival of the organisation, services or people. Dependence on interconnected activities using cyber platforms which might be private networks, cloud, web based services, mobile devices, as brought a new threat of catastrophic failures. There are also insider risks that may breach defences and geopolitical threats and consequences from world- wide events such as nuclear instability in DPRK which are covered in case study briefings in this course. The world-wide risks to the region's supply chains, energy security, transportation and important leisure industry will be discussed in the course. Successful application of catastrophic risk methods can grow the business by increasing the risk appetite for innovative and transformative projects. Entry into new markets and applications of new technology are challenges that may be made easier with the benefit of catastrophic risk knowledge.

Module 1: Catastrophic case studies and *Exercise Degradation*
Module 2: Risk matrix building and *Exercise Hotel Attack*
Module 3: Business risk model and *Case Studies*
Module 4: Risk intelligence and *Exercise Aviation and Port Attacks*

About the Instructor:
Dr. Sally Leivesley PhD Lond., MSPD, BA(Hons) Qld., FICPEM, FRSA, MACE, MIABTI, Director, Newrisk Limited and TEG7 LLP
Sally has a UK Home Office background and trained as a Scientific Advisor to respond to all aspects of nuclear attack and chemical, biological and radiological events. She plans, directs and participates in major exercises concerning critical components of industry and specialises in testing catastrophic threat impacts on critical functions of business. She has experience in all phases of risk assessment, planning, crisis management and post-loss recovery including psychological interventions in communities, post-disaster. Sally is a respected media adviser on public protection and is a member of the Register for Security Engineers and Specialists (RSES).

Details

Duration:	**2-day training course 2018**
London:	**2-3 July; 5-6 December**
Amsterdam:	**8-9 October**
Abu Dhabi:	**18-19 November**
Johannesburg:	**26-27 November**
Sectors:	**All**

Available as bespoke in-house training

For pricing and further information:

+44 (0)20 7936 8989 teampulse@pulseconferences.com www.pulseconferences.com