ENHANCING CYBER SECURITY IN THE PUBLIC SECTOR

LONDON, UK

Fee
£5,000

Fee inclusive of accommodation (single room), refreshments, luncheon, ground transportation and certificate awarded by The Queen Mary University of London.

Date
5-11 Nov. 2023

By joining
You get

A Visit To Relevant Agency in London

.....

QMUL

Certificate is awarded by the Queen Mary University of London

Introduction

CyberSpace is the frontier where fierce competition amongst organizations and nations. This highly contested space is critical for future development of nations. Its importance is premised on the exponential growth of the knowledge economy and Industry 4.0; pillared on the rising digitalization and the connectedness of the global community

The volume of data traffic in cyberspace is growing many folds, and is not expected to slow down. Security of this space is very critical for global and national development. However, the governance of this important space is very fluid and contentious and susceptible to huge risks. Protecting digital infrastructure in Critical National Infrastructure (CNI) is imperative to ensure continued delivery of public services.

It is therefore incumbent upon public policy makers, as custodian to the nation's governance system, to maintain an environment that minimize the risks from these threats to ensure integrity of our governance systems at all levels are protected. Emerging technologies will continue to pose challenges to existing systems; and understanding evolving issues becomes pertinent if we are to properly manage these threats.

Jointly organised by:

Queen Mary University of London

USM Universiti Sains Malaysia

APEX

PIPP A
PUSAT INOVASI DAN PRODUKTIVITI PENTADBIRAN AWAM
CENTRE FOR INNOVATION AND PRODUCTIVITY IN PUBLIC ADMINISTRATION
UNIVERSITI SAINS MALAYSIA

Course Contents

These Labs will explore the threats, the growing body of law and regulation and the best practice international standards that have developed to guide the policy response to the legal and operational risks relating to cybersecurity. Topics that will be addressed include:

Session 1:
Information Security and Technology: Introduction

Aims and purpose of the training course, the nature of information security/assurance: confidentiality, integrity, availability of information, need for information security, dependence on network systems, nature, scope of threats, concepts of trust, risk, governance

Session 2:
Information Security Laws and Regulations

Analysis of laws and regulations that provide direct/indirect legal imperatives to protect personal and other data including under: data protection statutes, private law, corporate governance responsibilities, consumer protection frameworks.

Session 3:
Sectoral Laws

Examination of sector specific laws and regulations governing information security in health, finance and telecommunications.

Session 4:
Standards, Certification and Codes

Proprietary and regulatory standards have emerged as benchmarks for 'reasonable' or 'adequate' measures of information security management, including ISO 27001 et seq. This session examines several of these standards and their core principles including risk classification and considers the legal import of standards and certification under them.

Session 5:
Security Breach Laws and Practice

There is a growing body of laws providing obligations to notify regulators and/or data subjects of information security breaches. The reality is that an information security breach is a matter of when and what and not if. This session explores these requirements and addresses some practical issues surrounding the planning for, detection and investigation of an information security breach.

Session 6:
National Security Concerns

Exploration of the concept of critical infrastructure and various EU and US frameworks, measures and standards to address its security, including the EU Network and Information Security Directive; institutional responses (e.g. ENISA & CERTs), the Wassanaar Agreement and Export Control regimes for technology with lawful and other uses.

Session 7:
Managing Risk: Corporate Strategies and Planning, Insurance, Employment Policies and Practice, Supplier Contracts

This session considers some practical ways in which organisations can effectively limit or manage the risk of cyber threats including policies to address, e.g., monitoring, BYOD, acceptable use of Internet, cloud computing TOS and due diligence.

Learning Outcomes

At the end of this programme, participants will better appreciate

- Latest technologies and tools to facilitate effective cyber security
- The legal and regulatory framework that supports cyber security
- The specific policy challenges of protecting CNI, including institutional responses (e.g. CERTs).
- Proprietary and regulatory standards of information security management, including ISO 27001
- Practical issues surrounding the planning for, detection and investigation of an information security breach.
- Good practices to manage risk to cyber threat

Trainer Profiles

Professor Anne Flanagan is a member of the Centre for Commercial Law Studies (CCLS). She convenes and lectures on LLM courses on EU Data Protection Law, Information Security and the Law and Telecommunications Law, as well as teaching similar courses on our distance learning LLM in Technology, Media and Telecommunications. She is a New York State licensed attorney. Before coming to Queen Mary, she practiced law for sixteen years as an associate with the law firm of Wilson, Elser, Moskowitz, Edelman & Dicker in New York and in the U.S. financial services industry. Her experience includes insurance regulatory compliance, appellate litigation and state government relations for providers of life, health and property/casualty insurance and pension products. Among her varied functions as Senior Counsel at TIAA-CREF, the world's largest private pension system, where she worked for seven years, Anne served as counsel to the IT divisions.

Professor Ian Walden is Professor of Information and Communications Law and Director of the Centre for Commercial Law Studies, Queen Mary, University of London. His publications include Media Law and Practice (2009), Free and Open Source Software (2013), Computer Crimes and Digital Investigations (2nd ed., 2016) and Telecommunications Law and Regulation (5th ed., 2018). Ian has been a visiting professor at the universities of Texas, Melbourne and KU Leuven. Ian has been involved in law reform projects for the World Bank, European Commission, Council of Europe, Commonwealth and UNCTAD, as well as numerous individual states. Ian was a 'expert nationaux détaché' to the European Commission (1995-96); Board Member and Trustee of the Internet Watch Foundation (2004-09); on the Executive Board of the UK Council for Child Internet Safety (2010-12); the Press Complaints Commission (2009-14), a member of the RUSI Independent Surveillance Review (2014-15) and is a member of the Code Adjudication Panel at the Phone-paid Services Authority. Ian is a member of the European Commission's Expert Group to support the application of the GDPR. Ian is a solicitor and Of Counsel to Baker McKenzie. Ian leads Queen Mary's qLegal initiative and is a principal investigator on the Cloud Legal Project.

Training Methodology

The program is designed to transfer knowledge, skills and experience in facilitator-led discussions, group activities and field trips to a relevant agency in London.

Who Should Attend

Designed for senior officials as well as decision-makers from public sectors and public linked companies with responsibility for cyber security.

How to register ? Complete the form below and email to: pippa@usm.my

No.	Name	Position	Mobile Phone	Email

Administration Details:

ORGANISATION : APPROVAL OFFICER :

ADDRESS :

PHONE : FAX : E-MAIL :

- Payment can be made via Cheque I Local Order I Bank Draft under the name of USAINS HOLDING SDN. BHD. and send to: Centre for Innovation and Productivity in Public Administration, Level 2, TORAY Building, USM, 11800 Pulau Pinang, Malaysia.
- PIPPA reserves the right to alter the programme schedule and details without prior notification. Fees quoted are subject to terms and conditions outlined in PIPPA's Registration Policy.
- Any cancellation made after confirmation letter has been issued by PiPPA, a 100% fees will be charged to the participants or to the organisations.
- Fees for cancellations / changes are calculated based on the total value of the booking.